DYNAMIC STATE ESTIMATION BASED PROTECTION SCHEME FOR CYBER-ATTACKS ON MICROGRIDS

A Dissertation
Presented to
The Academic Faculty

By

Orestis Vasios

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
School of Electrical & Computer Engineering

Georgia Institute of Technology

May 2022

DYNAMIC STATE ESTIMATION BASED PROTECTION SCHEME FOR CYBER-ATTACKS ON MICROGRIDS

Thesis committee:

Dr. A. P. Meliopoulos, Advisor
School of Electrical & Computer Engineering
Georgia Institute of Technology

Dr. Santiago C. Grijalva
School of Electrical & Computer Engineering
Georgia Institute of Technology

Dr. Raheem A. Beyah
School of Electrical & Computer Engineering
Georgia Institute of Technology

Dr. Nagi Z. Gebraeel
School of Industrial & Systems Engineering
Georgia Institute of Technology

Dr. Maryam Saeedifard
School of Electrical & Computer Engineering
Georgia Institute of Technology

Date approved: January 14, 2022

To Nefeli, Mairi and Nikos

ACKNOWLEDGMENTS

During the Ph.D. marathon, I was lucky to receive support from a large group of people. This journey would not have been successful without them, and for this I will be forever grateful.

First and foremost, I would like to express my sincere gratitude to my advisor, Prof. Sakis Meliopoulos, for offering me the opportunity to join the Power Systems Control and Automation Laboratory (PSCAL) and for investing countless hours in teaching me ever after. His advice on both technical matters as well as on how to properly and professionally conduct research has been invaluable and his energetic personality and tirelessness continue to be a source of inspiration. I would not have become the researcher and person I am today without him. For this, I will be forever indebted.

I would also like to thank my Ph.D. committee members, namely Prof. Raheem A. Beyah, Prof. Maryam Saeedifard, Prof. Santiago C. Grijalva, and Prof. Nagi Z. Gebraeel for their constructive suggestions and advice that helped improve this dissertation. Their time and effort are really appreciated.

Some of my best memories from the Ph.D. journey came while I was teaching our undergraduate students; a big honor and even bigger responsibility. I cannot thank Dr. Joy Harris enough for her trust and for being an amazing mentor, as well as a source of support during challenging moments.

The foundation of my academic efforts was laid while I was a student at the National Technical University of Athens in Greece. I would particularly like to thank Professor Nikos Hatziargyriou and Professor Costas Vournas for all the important lessons I received from them and for still being there for me.

I am also grateful for the opportunity to intern at the Argonne National Laboratory during my studies. I would particularly like to thank Dr. Dongbo Zhao, Dr. Yuting Tian, and Dr. Tianqi Hong for their efforts and commitment to provide me with a fruitful and productive collaboration in the midst of the global COVID-19 pandemic.

I would not have finished this dissertation without the collaboration, advice and help of my fellow students and friends at the PSCAL. Special thanks to Dr. Hussain Albinali for introducing me to power system protection concepts, and to Dr. Boqi Xie for the countless hours we spent together debugging code. I am also grateful for collaborating with Stella Kampezidou, Juan C. Lazarte, Dr. Mohit Srinivasan, Dr. Maad Alowaifeer, Kaiyu Liu, Dr. Chiyang Zhong, and Dr. Jiahao Xie, as well as Dr. Evangelos Polymeneas, Dr. Abdullah Alamri, Dr. Liangyi Sun, Dr. Yu Liu, Dr. Rui Fan, Dr. Bai Cui, Dr. Chanyeop Park, and Gad M. Ilunga. Moreover, I am deeply thankful for my close friends from outside PSCAL, namely Dr. Sadegh Vejdan, Dr. Kavya Ashok, Dr. Shreyas Kulkarni, Steven Moore, Mickaël Mauger, Dr. Evgeniya Tsybina, and Dr. Rohit A. Jinsiwale. The moments we spent together made the Ph.D. journey much more enjoyable!

A list of people like this could never be complete without the friends who were my second family in the US. Artemis Boulamatsi, Nikos Sarafianos, Giorgos Boutselis, Nikos Spilias, Eva Kallou, Thanasis Kountouras, Xenophon Konstantinou, Grace Yu, your presence and friendship during all these years meant the world to me!

And as a testament to how deep bonds can stand the test of time and of seven time zones of distance, I am extremely grateful for Michalis Avgoulis, Vasiliki Koniakou, Thanasis Gkikas, Nikos Reppas, Petros Agriomallos, Katerina Korakianitou, Nikolas Korasidis, Stavros Aronis, Tasos Kamateros, and Dimitris Koutsoukos.

Finally, none of these adventures would have been possible without my sister, Nefeli Vasiou, and my parents, Mairi Kollia and Nikos Vasios. This work is dedicated to them.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

CISA Cybersecurity and Infrastructure Security Agency

CT Current Transformer

DER Distributed Energy Resource

DFT Discrete Fourier Transform

DHS US Department of Homeland Security

DMS Distribution Management System

DOE US Department of Energy

DOJ US Department of Justice

DoS Denial-of-Service

DSE Dynamic State Estimation

FDIA False Data Injection Attack

GPS Global Positioning System

ICS Industrial Control System

IED Intelligent Electronic Device

IT Information Technology

KCL Kirchhoff’s Current Law

KVL Kirchhoff’s Voltage Law

MCIA Malicious Command Injection Attack

PCC Point of Common Coupling

PMU Phasor Measurement Unit

SCAQCF State and Control Algebraic Quadratic Companion Form

SCQDM State and Control Quadratized Device Model

SPWM Sinusoidal Pulse Width Modulation

WLS Weighted Least Squares

SUMMARY

In recent years, news about cyber-attacks targeting critical infrastructure has been increasing at an alarming frequency. Systems that have been targeted include the healthcare sector, water supply systems, and, of course, the power grid. These are areas where systems play a vital role in the normal operation of a modern society. As such, cyber-attacks have understandably become a source of worry for the general public.

In terms of power grids, there are reasons for lasting concern as well as recent positive developments. First, the main challenge with the protection of the power grid from cyber-attacks is that the relevant infrastructure has been built over many decades, and investments in equipment are expensive, so installed equipment is usually expected to last for a considerable amount of time. Therefore, parts of the system may become outdated and vulnerable to cyber-attacks. Moreover, the power grid is a complex system covering huge geographic areas, and is controlled, maintained and operated by many different stakeholders with different areas of responsibility, posing serious coordination challenges when attempting to update the infrastructure. However, there have also been encouraging developments in the recent past. The most important one is the general increase in computational power, which has also translated to considerable gains for the equipment that is used to monitor power systems, such as microprocessor-based relays. Furthermore, the power grid has benefited significantly from improvements in communications equipment. Among other things, there has been a considerable expansion of modern communications infrastructure such as fiber optic cables.

In this environment, many challenges, vulnerabilities, and points of concern remain. This dissertation mainly focuses on false data injection attacks, i.e., scenarios where a malicious actor manages to falsify system measurements aiming to confuse or trick either monitoring equipment or system operators regarding the system state and operation. By spoofing power system measurements, adversaries can give a false impression of the system

operation and have legitimate control functions or people operating the system react by taking actions that severely disrupt a system that would otherwise operate properly.

This dissertation introduces a novel microgrid protection scheme that addresses such concerns by analyzing system measurements and identifying measurement falsification attempts within a microgrid. The proposed scheme is responsible for the supervision of all relays that monitor individual protection zones of the protected microgrid. In order to achieve its goal, it operates in a centralized manner by receiving and analyzing measurements recorded throughout the microgrid.

The three main reasons why microgrids were selected for this dissertation are a) their rising importance for future power grids, b) the high likelihood of already having a centralized way of recording measurements and estimating the microgrid state, which means that the introduced scheme adds only a reasonable computational overhead, and c) the high likelihood of having installed communications infrastructure, aided in particular by the fact that they usually cover relatively small geographical areas.

The operation of the microgrid protection scheme that is introduced in this dissertation can be summarized in the following manner. The introduced scheme a) continuously receives measurements that are either already in phasor form, or are recorded in the time domain but can be converted to phasor form, b) builds a microgrid model according to a modular approach that uses detailed object-oriented descriptions of individual devices to rapidly form the microgrid level model automatically, c) performs Dynamic State Estimation (DSE) in the phasor domain to estimate the microgrid state at least once per cycle and possibly even more frequently than that, d) computes the microgrid confidence level, which is an indicator of whether the recorded measurements fit the microgrid model, and e) uses the confidence level to declare that either the microgrid operation is proper, or that an abnormality has been detected.

In case of abnormality detection, the introduced microgrid protection scheme performs hypothesis testing. During this procedure, it identifies a suspect measurement utilizing

the normalized residuals calculated during DSE, and identifies whether the removal of one of the following options leads to an acceptable confidence level when DSE is performed again, thus identifying the cause of the abnormality. The options considered here are a) the removal of the suspect measurement alongside every other measurement from the same measuring device, b) the removal of the suspect measurement alongside every other measurement from the same protection zone, or c) the removal of the suspect measurement alongside every other measurement from the same measuring device and the same protection zone.

If a fault is detected by the hypothesis testing procedure, the scheme allows the protective relays of the affected zone to immediately trip its breakers. In any other case, breaker tripping must be prevented in order to maintain proper operation. At the same time, if the cause of the detected abnormality is classified as a measurement spoofing attack, the system operator must be immediately notified.

The introduced protection scheme is tested on two different microgrids that differ in size and level of individual device modeling detail, and its proper operation is confirmed.

The main contribution of this dissertation is the development and testing of a novel protection scheme that a) defines an object-oriented syntax suitable for the detailed mathematical description of any microgrid device model in both the time and the quasi-dynamic domains, b) includes a classification system that labels each measurement within a microgrid based on its corresponding protection zone and recording device, c) converts time domain measurements to phasors, if necessary, d) defines an automated process to create a high-fidelity microgrid measurement model based on knowledge of individual device models and microgrid topology, e) contains a flexible object-oriented DSE module that calculates the goodness of fit of recorded measurements to the microgrid measurement model, f) detects abnormalities that may exist based on goodness of fit, and g) identifies suspect measurements, if an abnormality is detected, and uses the measurement classification system and the flexible DSE module to identify the cause of the abnormality.

CHAPTER 1
INTRODUCTION

One of the most serious challenges facing modern power systems is the threat of cyber-attacks able to disrupt their normal operation. This dissertation proposes a method to detect intruders who obtain unauthorized access to electronic devices installed in microgrids, and interfere with the measurements these devices record. As the proper control of any microgrid relies on knowledge of its true operating state, such attacks are a source of significant concern for healthy microgrid operation.

1.1 Background

The proliferation of cyber-attacks targeting critical infrastructure poses a serious challenge to the provision of crucial services to society. In 2018, the city of Atlanta, where the Georgia Institute of Technology (Georgia Tech) is located, experienced a ransomware attack that led to the shutdown of important municipal services ranging from the water bill payment system to the public Wi-Fi at the Hartsfield-Jackson Atlanta International Airport [1, 2].

During the writing of this dissertation, Atlanta was once more at the epicenter of US attention because of a cyber-attack. This time, the Colonial Pipeline, which is partly located in the Atlanta metropolitan area [3], was shut down due to a ransomware attack [4] causing panic and fuel shortages at gas stations along the East Coast [5]. Shortly after the attack, President Biden issued an "Executive Order on Improving the Nation's Cybersecurity" [6], and Reuters reported that the US Department of Justice (DOJ) elevated ransomware attack investigations to the same priority level as terrorism investigations [7].

Other recent attacks on critical infrastructure include reported attacks on water supply systems in Florida [8] and California [9], which could have lead to widespread poisonings throughout the areas served by the affected systems if not stopped in time. Healthcare providers have also been targeted, most notably during the notorious WannaCry cyber-attack in 2017, which caused widespread problems in the UK [10], or, more recently, in the US in 2020 [11] and Ireland in 2021 [12]. These attacks lead to delays or cancellations for a wide range of medical procedures including cancer treatment.

Incidents such as the ones previously described have increased both the public interest and the intensity of research efforts in the field of cybersecurity. However, these are not the sole examples of disruptions to civilian life by malicious actors.

The power grid, a critical infrastructure supporting numerous functions of everyday life, has also been a target of multiple cyber-attacks. The December 2015 attack on the Ukrainian power grid is probably the most famous example worldwide of a successful cyber-attack on a power system[13]. Roughly 225,000 customers lost power during this attack for intervals lasting up to several hours. Despite its unprecedented size (at least compared to other attacks for which details are publicly available), this attack may have been dwarfed in October 2020. Then, the Indian city of Mumbai experienced a blackout that affected millions of customers in this metropolitan area of roughly 20 million people. In parts of the affected area, it lasted for more than 12 hours [14]. Reports allege that the blackout may be the result of a cyber-attack [15], although no conclusive report seems to have been publicized yet.

As far as individual power plants are concerned, probably nothing worries the general public more than a catastrophic failure at a nuclear facility. Fortunately, no cyber-attack has resulted in such an event so far. Nevertheless, malware has indeed been detected in nuclear power plants in Germany in 2016 [16] and in India in 2019 [17]. Moreover, computer systems in at least twelve US power plants, including the nuclear Wolf Creek Generating Station, were compromised according to 2017 reports [18]. While these attacks did not interrupt the power generation from the affected nuclear plants, the US Department of Homeland Security (DHS) reported that a cyber-attack against a turbine control system in October 2012 halted the operation of a power plant for three weeks [19].

The increase in the number of attempts to electronically attack the power grid has also led to many initiatives aiming to improve its defense.

In the United States, the US Department of Energy (DOE) released a comprehensive Cybersecurity Strategy for 2018-2020 in June 2018 [20]. According to this document, the DOE should accomplish four goals, namely a) delivery of high-quality Information Technology (IT) and cybersecurity solutions, b) continuous improvement of its cybersecurity posture, c) change from IT owner to IT broker to improve customer focus, and d) excellence in the stewardship of taxpayer dollars.

In April 2021, the DOE, alongside partners from the electricity industry and the Cybersecurity and Infrastructure Security Agency (CISA), launched a 100-day plan aiming to improve the cybersecurity of the power grid [21]. The goals of this plan are a) modernization of protections against cyber-threats, b) encouragement of adoption of technology that helps identify, protect against and investigate cyber-attacks, c) improvement of situational awareness and response capabilities in essential Industrial Control Systems (ICSs) according to specific targets within the 100-day interval, d) improvement of cybersecurity capabilities of critical IT networks, and e) deployment of technology to identify cyber threats in ICSs on a voluntary basis.

In the European Union, the European Commission adopted a Commission Recommendation in April 2019 [22] instructing member states to a) apply up-to-date security standards on new installations and improve old installations, where necessary, b) apply appropriate standards for cybersecurity and secure real-time communication, c) consider real-time security constraints for assets, d) consider using high-quality communication networks, e) split the power system into logical zones to enable appropriate cybersecurity measures, f) choose secure communication protocols, g) introduce suitable authentication mechanisms, h) install only new devices (including Internet of Things devices) that are appropriately secure, i) consider cyber-physical effects in business plans, and j) meet the design criteria for a resilient grid.

As noted in the examples above, it is clear that power grids are attractive targets for cyber-attacks due to modern society's needs for uninterrupted electricity supply. As such, research efforts in this area are essential for system operators to protect themselves from malicious parties.

1.2 Research objective

While cybersecurity methods that are developed to protect computers and computer networks in general can also be applied to the digital infrastructure of the power grid, the fact that power systems are cyber-physical systems offers additional capabilities.

The objective of this dissertation is the development of a comprehensive centralized protection scheme for microgrids to guard against cyber-attacks by utilizing Dynamic State Estimation (DSE) in the quasi-dynamic domain [23, 24, 25]. This system complements the individual relays installed in the microgrid, each of which is responsible for a specific protection zone. These individual relays are tasked with tripping the appropriate breakers if they detect that a system component is operating abnormally within their monitored protection zone. The presented protection scheme utilizes the set of all the measurements that are received by individual relays in order to identify whether a detected abnormality can be attributed to an actual fault in the system, or whether it is a result of a cyber-attack that aims to cause the tripping of a healthy protection zone. If the latter is true, the protection scheme prevents the appropriate individual relay from erroneously tripping a healthy portion of the power grid.

This research work builds on an already extensively researched framework that utilizes DSE to accurately estimate the operating state of a selected part of the power grid based on the measurement of appropriate physical quantities. Then, a statistical test is used to decide whether the operating state of the monitored area fits the corresponding physical model to detect possible abnormalities with high probability. The result of this framework is a new type of relay called settingless due to the minimal number of required settings compared to legacy relays. Instead, settingless relays identify faults by detecting abnormal operating conditions [26, 27, 28, 29]. The proposed scheme also draws from two other relatively recent developments in the field of power systems. First, the introduction of Distributed Energy Resources (DERs) in large numbers in distribution systems has accelerated the adoption of microgrids, which are logical subdivisions of the power grid that can operate autonomously or interconnected to the rest of the grid. Standardization efforts for DER interconnection further enable this process [30]. Second, new standards like IEC 61850 streamline the communication of Intelligent Electronic Devices (IEDs), thus enabling the deployment of a large number of them to monitor the power system and measure all physical quantities of interest.

The proposed scheme uses these technological advances to detect not only the abnormal operation of a microgrid due to some electrical fault, but also abnormalities in measurement data that can be attributed to a data cyber-attack. Since the proposed scheme tests the goodness-of-fit of the acquired measurements and microgrid model, special emphasis is placed on the modeling of microgrid devices. Such models should capture all the details of the physical operation of a device without simplification. They should also be object-oriented for two main reasons. First, modularity is crucial, as the configuration of a microgrid frequently changes. Second, the object-oriented nature of these models enables a distributed computational approach that increases the computational efficiency of the proposed scheme.

1.3 Thesis outline

The rest of this thesis is organized as follows.

Chapter 2 offers a review of the literature on known cybersecurity incidents that have affected power systems around the world, provides a categorization of cyber-attacks that may affect the power grid, and summarizes proposed defense mechanisms against such attacks. Chapter 3 describes the novel protection scheme that is introduced in this thesis, and explains how it can protect microgrids from cyber-attacks. Chapter 4 outlines an object-oriented modeling approach that can describe any microgrid device, as well as any microgrid as a whole. This approach emphasizes flexibility and modularity and enables the proper operation of the novel protection scheme. In Chapter 5, the object-oriented modeling approach of Chapter 4 is utilized in order to extract a measurement model for any microgrid. Moreover, additional measurement types are introduced in order to improve the performance of the proposed protection scheme. Chapter 6 analyzes the core of the introduced protection algorithm. This algorithm relies on quick and accurate dynamic estimation of the microgrid state based on recorded measurements, and evaluates whether the recorded measurements fit the microgrid model with a reasonable level of confidence. If a mismatch is detected, a hypothesis testing approach is proposed to identify the reason. Chapter 7 demonstrates the successful application of the novel protection method on two microgrids. Finally, Chapter 8 concludes this dissertation, summarizes its main contributions, and suggests possible paths for future research.

Appendix A demonstrates the necessary steps to model a transformer according to the modeling approach of Chapter 4 starting from a schematic of the transformer equivalent circuit. In Appendix B, the concept of a synchrophasor is presented alongside the algorithm used in this thesis to estimate synchrophasors from available measurements in the time domain. A brief review of the literature on synchrophasor estimation is also included.

CHAPTER 2
LITERATURE REVIEW

This chapter offers a review of research efforts in the area of power system cybersecurity. First, the most important known cyber-attacks are presented. Then, a categorization of different types of cyber-attacks is offered, followed by information on defense measures that have been deployed or developed.

2.1 Real-life cybersecurity incidents

The Aurora Generator Test, which was conducted by the Idaho National Laboratory in 2007, was probably the first widely publicized demonstration of the capability of a cyber-attack to seriously disrupt the normal operation of the power grid [31]. Although the destruction of the targeted electric generator happened within a controlled lab environment, this test only predated the detection of what is considered to be the first deployed cyber-weapon ever, Stuxnet, by only three years [32]. Stuxnet was apparently used to destroy centrifuges used for uranium enrichment within the Natanz Nuclear Facility in Iran. While these centrifuges were not part of the Iranian power grid, the controllers targeted by Stuxnet can also be used for power applications. Finally, the first publicized wide-scale attack on a power system was launched in December 2015 against the Ukrainian power grid affecting approximately 225,000 customers [13]. This specific attack was focused on the distribution system and hit three different regional distribution system operators. The full restoration of the power grid to normal operation was accomplished after several hours.

These events are publicly reported and thoroughly analyzed by technical investigators. However, due to government or corporate secrecy many more cyber-attacks or attempted cyber-attacks have either remained unknown to the general public or have been reported only by general news media outlets omitting most of the technical details. This list includes additional suspected cyber-attacks in Ukraine [33, 34] and the United States [35], as well as a possible intrusion of US agencies into the Russian power grid [36]. Thus, it is hard for the academic community to have accurate information on real-life incidents or available cyber-attack capabilities.

The attackers in both real-world events described in this section utilized generally applicable techniques, such as zero-day vulnerabilities of the Windows operating system [37] or vulnerabilities of the Microsoft Office suite [13], as part of their attack. However, due to the breadth of the bibliography on general cybersecurity research, the scope of the rest of the literature review will be narrower, focusing only on issues directly applicable to the power grid. The specific vulnerabilities of parts of the modern power grid should be taken into consideration during the design and operation of any power system [38].

2.2 Classification of cyber-attacks targeting the power grid

The two main types of possible cyber-attacks on the power grid are Denial-of-Service (DoS) attacks and data attacks. Data attacks include Malicious Command Injection Attacks (MCIAs) and False Data Injection Attacks (FDIAs) [39]. It should also be noted that attackers that compromise parts of the power grid may elect to passively record communications and extract sensitive information, usually in order to better prepare for an attack [39].

DoS attacks may disrupt the normal operation of power systems, especially microgrids, by making needed components like routers or communication links totally unresponsive [39] or by delaying messages beyond the requirements imposed by the real-time operating constraints of system components [40]. Therefore, important information on the operating state of the power system or issued control commands may never reach the appropriate destination. Moreover, the widespread adoption of wireless networks as the main means of internal communications particularly in microgrids also makes jamming a potent tool to implement DoS attacks. Regardless of the communications technology used though, attackers may also perpetrate DoS attacks by infecting installed IEDs and instructing them to start flooding the communications infrastructure with messages that contain no useful information [39].

Malicious command injection is the most obvious way that the power grid may be attacked. All three real-world examples presented in the previous section fall into this category. In the case of Stuxnet, the malicious code made the controllers of the centrifuges to operate them in a way that would physically damage them [32]. In the case of the attack on the Ukrainian power grid, the attackers remotely instructed substation breakers to open causing outages for thousands of customers [13]. Moreover, during the Aurora Generator Test, the generator breakers were opened and closed out of synchronism in order to destroy the generator [31].

Finally, FDIAs can affect the power grid in multiple ways. Their effect on state estimation has been widely researched and some of the possible events are economic attacks, load redistribution attacks, and energy deceiving attacks. Economic attacks can manipulate the Locational Marginal Price (LMP) at different system nodes, possibly enabling the attacker to extract financial gain. Load redistribution attacks may force the system to operate in an uneconomic state. More importantly, they may make the system shed load to meet security constraints, thus causing outages to customers, or even overload a line to cause physical damage if its protection system fails to operate. Moreover, energy deceiving attacks may lead to a mismatch between power demand and supply [41]. FDIAs can also lead to instability in the operation of a microgrid or cause nodes to try to converge to voltage values that would trigger the overvoltage protection function to disconnect them from the system [42]. The common thread linking all these kinds of attacks is that attackers manipulate measurements to force the legitimate control and protection functions to react and issue commands that satisfy the attackers' goals.

2.3 Mitigation and protection against cyber-attacks targeting the power grid

There is a wide array of general-purpose defenses that can be deployed against cyber-attacks. One possible approach would be to define new networking architectures that would increase the resiliency of power grid communications to cyber-attack by focusing on a) self-healing communications management, b) communications network verification, and c) intrusion detection [43]. General intrusion techniques that detect different types of cyber-attacks, assess their severity, and distinguish them from conventional power faults have also been proposed [44].

Specific defense mechanisms against DoS attacks may aim to either strengthen the communications of the power grid or enable some form of coordination between the installed devices in the absence of communications. The first category contains methods such as the one that attempts to guarantee the fulfillment of timing requirements in the presence of any potential jamming attack against wireless power system communications [40]. Alternative control techniques that can be activated after the loss of communications to keep the power grid functioning until the restoration of communications fall under the second category [45].

FDIAs differ in the type and amount of information available to the attackers to recreate the system state, as well as the number and exact location of the measurements that can be compromised [41]. Therefore, the main defense mechanism against them is based on the protection of the minimal set of critical measurements that are sufficient for the accurate reconstruction of the system state, possibly through the use of devices more resistant to cyber-attack like Phasor Measurement Units (PMUs) [41]. In order to achieve this goal at the minimum effort and cost, the careful selection of the measurement devices to be protected is very important. It should be noted that PMUs are more resistant to cyber-attacks, but there are still ways to attack them, mainly through Global Positioning System (GPS) spoofing [46]. A minimal set of PMUs that still makes the system observable can offer measurements that can be statistically analyzed for consistency in order to reveal FDIAs, if the aforementioned PMUs are not compromised [47]. Such techniques rely on the accumulation of measurements from different PMUs in a central location for state estimation to be performed. However, extensions exist that try to achieve the same result in a distributed manner without running state estimation, which is useful in the case of microgrids lacking a central management system [42, 48]. For AC systems, FDIAs also differ based on whether the attackers utilize DC or AC power flow solutions to calculate their attack. The former are simpler to analyze and more extensively researched [41, 47] but also easier to detect by system operators using AC state estimators [49]. More research has been done in this area including the use of authentication schemes for data packets, low rank matrix factorization, and the wider deployment of meters on the user side [41].

Machine learning techniques have also been demonstrated both for general use and as tailored countermeasures to specific types of attack. The research literature contains examples that use Support Vector Machines (SVMs) [50, 51], Non-Nested Generalized Exemplars (NNGEs) [52], Density Ratio Estimation (DRE) [53], Neural Networks (NNs) [54], and Reinforcement Learning [55].

However, none of the reviewed mitigation efforts appears to work directly with the protection functions of a power system in order to prevent them from erroneously tripping healthy portions of the grid, as they all focus on different areas of the operation of a power system.

2.4 Summary

This chapter presented the best known examples of publicized cyber intrusions that affected power grids and other similar infrastructure. Moreover, possible cyber-attacks against power systems were classified into DoS attacks and data attacks, and an overview of implementations of such attacks was offered. Then, a review of proposed schemes to protect power grids from each of these cyber-attack categories was provided. It should be noted that none of the reviewed protection schemes appears to work directly at the power system protection level, and this thesis aims to address this research gap.

CHAPTER 3

PROTECTION SCHEME OVERVIEW

Microgrids, like all power systems, are divided into individual zones for protection purposes. One or more relays receive current, voltage, and other measurements from each zone, perform the required calculations for the implemented protection functions, and detect power faults accordingly. Upon detection of a fault, appropriate action should be taken to disconnect all affected parts of the system. Speed is very important here in order to protect people from harm and equipment from damage, so protection schemes need to be automated and reach decisions very quickly based on available measurements. This situation is ripe for an attacker to exploit by tampering with some measurements in order to trick the protection scheme into believing that a fault has indeed happened. The protection scheme would then proceed to disconnect devices that are operating normally, and thus possibly disconnect critical loads needlessly. The novel scheme introduced in this dissertation works centrally at the microgrid level, possibly as a part of a controller that implements every function necessary for the safe and optimal operation of the microgrid [56]. It collects measurements from all individual zones and processes them according to the algorithm presented in this chapter with the goal of preventing this type of cyber-attack.

3.1 Protection algorithm

The flowchart shown in Figure 3.1 describes the basic steps of the novel protection algorithm. Figure 3.2 shows the internal operation of the hypothesis testing module. Here, the minimum acceptable confidence level is denoted as c_t. The choice of a specific c_t value is left to the discretion of the microgrid operator. It is usually good to pick a c_t between 50% and 80%, and the numerical experiments for this thesis adhere to this rule.

The implementation of the proposed centralized protection scheme requires an accurate

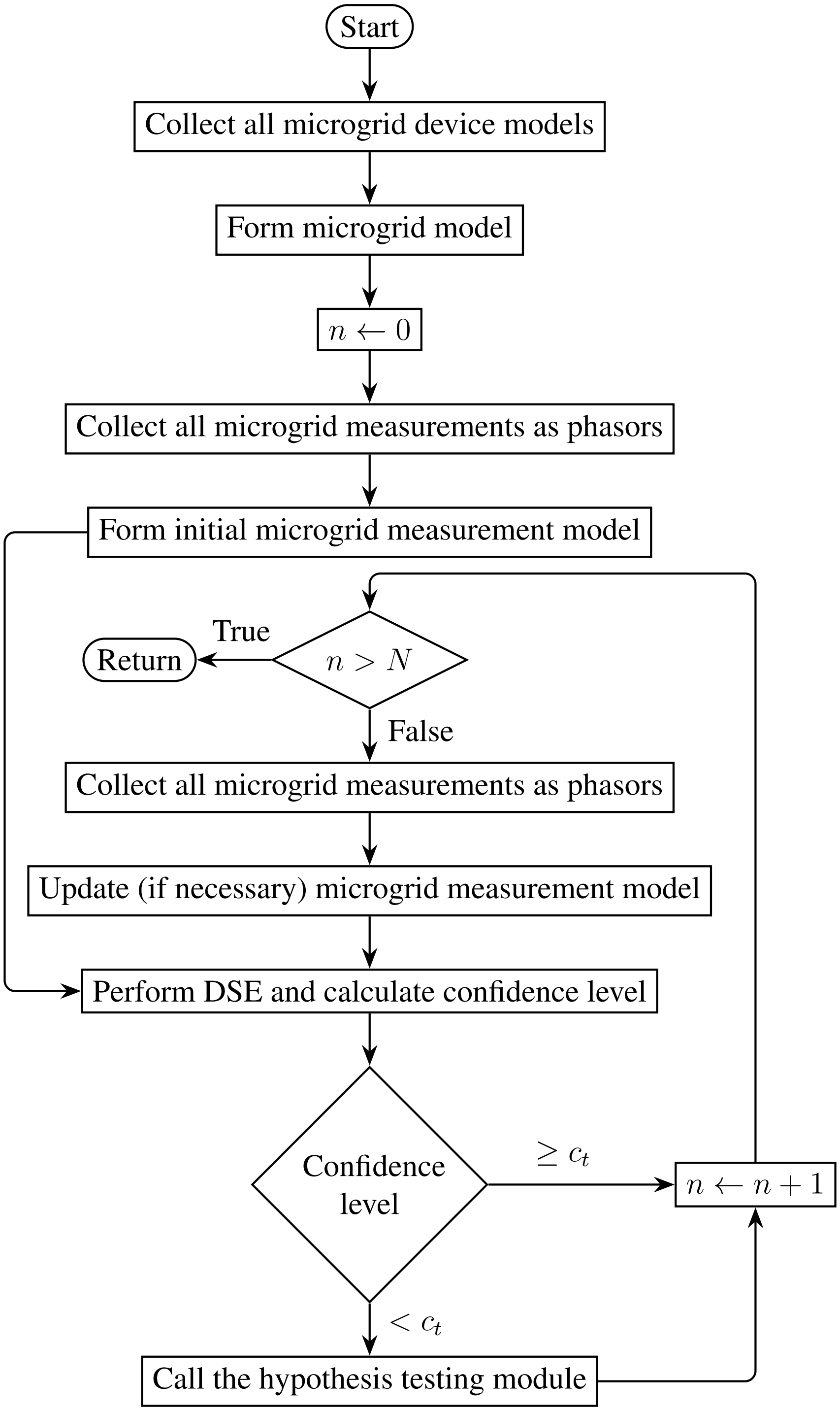
Start
Collect all microgrid device models
Form microgrid model
$n \leftarrow 0$
Collect all microgrid measurements as phasors
Form initial microgrid measurement model
True
Return
$n > N$
False
Collect all microgrid measurements as phasors
Update (if necessary) microgrid measurement model
Perform DSE and calculate confidence level
Confidence level
$\geq c_t$
$n \leftarrow n+1$
$< c_t$
Call the hypothesis testing module

Figure 3.1: Overview of the protection algorithm.

timestamp for each measurement to facilitate time synchronization. This requirement is easily achieved, since accurate timestamping is a common capability of modern IEDs with the timing signal usually provided by a GPS clock.

The first step during each iteration of the algorithm is the collection of measurements that are continuously recorded and streamed from all available measuring devices. Measurements for a single quantity (usually a single-phase current or a single-phase voltage) from a specific IED form a measurement channel. This means that each measuring device streams multiple measurement channels, and also that the same quantity can be measured by multiple measurement channels for redundancy purposes.

The protection algorithm introduced in this dissertation works on the quasi-dynamic domain, thus relying on phasor quantities for its implementation. Each measurement channel can directly stream timestamped phasors, which are also known as synchronized phasors or synchrophasors [57, 58]. This can be achieved with measuring devices called PMUs. However, in many cases the available IEDs stream instantaneous measurements. The introduced algorithm accounts for this, as it includes a Discrete Fourier Transform (DFT)-based phasor extraction module. Thus, for each stream of measurements received through a measurement channel, the corresponding synchrophasor can be calculated, if necessary.

It should be noted that there exists a wide array of algorithms for synchrophasor extraction, so there is considerable flexibility in the choice of the algorithm to be implemented, each with their own characteristics and strengths. One of the more important characteristics is the length of the calculation window, as these algorithms depend on measurements taken over some time interval.

A more thorough discussion of time synchronization, synchrophasors, and phasor extraction is provided in Appendix B.

Subsequently, the DSE algorithm needs to be executed. The main prerequisite for this step, apart from the obtained measurements, is an accurate, high-fidelity microgrid model, because the proposed approach relies on verifying that the measurements fit a quasi-dynamic model of the microgrid. In this dissertation, an object-oriented procedure is presented as a means of standardizing individual microgrid device models. Modularity is one of its crucial characteristics, as it increases computational efficiency, while also enabling the flexibility needed for microgrids that may frequently change their topology. Thus, this procedure ensures that the microgrid model can be quickly changed every time that a device is connected or disconnected. Chapter 4 provides detailed information about the device modeling process.

Individual device models need to be further combined in order to form a microgrid model. An algorithm that automates this process is provided in Chapter 5. This algorithm utilizes the attractive characteristics of the individual device modeling approach such as modularity to maintain a low computational burden. Chapter 5 also provides the necessary steps to produce a model that describes the microgrid measurement equations based on the microgrid model.

After the creation of an accurate microgrid measurement model, the obtained synchronized phasors are combined with it in order to perform DSE through the Weighted Least Squares (WLS) method. This step produces an estimate for the system state. Once this estimate is calculated, it is fed back to the microgrid measurement model equations in order to provide estimates for the recorded synchrophasors. Afterwards, the chi-square test is utilized to calculate the confidence level, i.e., the probability that the discrepancies between phasor estimates and phasor measurements are statistically important, which shows whether the measured synchrophasors fit the microgrid model.

A substantial drop of the confidence level, both in magnitude and in duration, implies that the microgrid operates abnormally. However, the reason why the obtained measurements do not fit the system model is important. An actual fault in the system should be cleared immediately. On the other hand, the drop of the confidence level may be attributed to erroneous measurements. Specifically, an attacker may gain access to one or more IEDs, and alter the acquired measurements. The proposed scheme can detect such an attack and block the relay that is responsible for the affected zone from tripping based on the modified measurements.

The confidence level calculation procedure, as well as the abnormality identification procedure, are analyzed in Chapter 6.

3.2 Hypothesis testing

Different hypotheses must be tested to distinguish cyber-attacks from faults every time that a confidence level drop is detected. These are a) a compromised instrumentation channel transmitting erroneous measurements, b) a power fault in a single device within the protection zone, and c) a combination of the two previous hypotheses. It should be noted that an instrumentation channel in this context is a group of measurements with a common source, i.e., a group of measurement channels recorded by the same measuring device.

The hypothesis testing part of the proposed scheme relies on the normalized residuals calculated during the DSE phase of the algorithm. A residual is the difference between the actually recorded measurement corresponding to some system quantity and the estimated value for the same quantity. The estimated value is computed using the model equation that describes this specific quantity and the system state calculated through DSE. A normalized residual is simply a residual divided by some normalization factor. In this dissertation, the standard deviation of a measurement is used as its normalization factor, as well as its weight for WLS purposes.

As is evident from the definition of a normalized residual, an unusually high value (in absolute value terms) indicates an unusually high distance between the measurement for a quantity and its estimated value. Therefore, utilizing normalized residuals to detect suspect measurements is a promising approach for hypothesis testing. In this dissertation, every time that the confidence level drops substantially during DSE, the absolute value of every normalized residual is calculated, and a list of measurements in descending order of absolute normalized residual is created. Afterwards, the measurement with the largest absolute normalized residual is considered suspect, thus triggering the hypothesis testing process. The flowchart in Figure 3.2 describes the logic of this process.

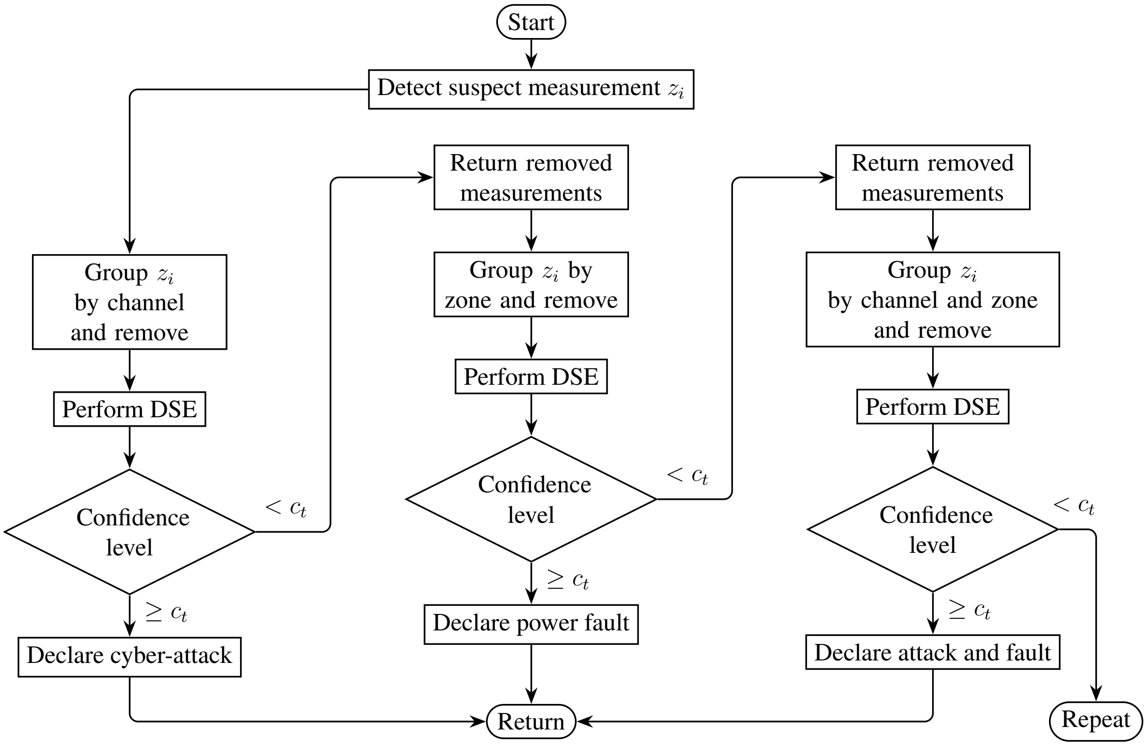

Figure 3.2: Overview of the hypothesis testing part of the protection algorithm.

The first goal of the hypothesis testing process is the determination of whether a cyber-attack may have occurred. In order to achieve this, all recorded measurements emanating from the same instrumentation channel as the suspect measurement are removed from the pool of measurements. In turn, this necessitates an update of the microgrid measurement model in order to remove the corresponding measurement equations. Then, the DSE part of the algorithm is repeated. The execution of DSE essentially as a subroutine of the hypothesis testing process demonstrates the importance of modularity in the design of the introduced protection approach. Furthermore, it is worth stating here that a high level of measurement redundancy is necessary in order to enable this step without impairing the DSE execution.

In a modern microgrid, this is a reasonable requirement, as there are many IEDs that can potentially stream measurements to the proposed centralized scheme. Apart from the actual recorded measurements, Chapter 5 introduces additional measurement types based on microgrid topology, which are called derived, virtual, and pseudo measurements. This increases the total number of measurements, which improves the performance of the DSE.

The number of IEDs that can be installed in a microgrid alongside the derived, virtual, and pseudo measurement types help achieve high levels of redundancy in the system to satisfy the observability requirement. Specifically, there must be enough independent measurements to reconstruct the state vector. For linear time-invariant (LTI) systems, observability can be proven using the observability matrix. An LTI is described as follows.

$$\dot{\mathbf{x}}(t) = \mathbf{A}\mathbf{x}(t) + \mathbf{B}\mathbf{u}(t) \tag{3.1}$$

$$\mathbf{y}(t) = \mathbf{C}\mathbf{x}(t) + \mathbf{D}\mathbf{u}(t) \tag{3.2}$$

Then, the observability matrix is

$$\mathcal{O} = \begin{bmatrix} \mathbf{C} \\ \mathbf{CA} \\ \mathbf{CA}^2 \\ \vdots \\ \mathbf{CA}^{n-1} \end{bmatrix}. \tag{3.3}$$

where n is the total number of states. If the rank of matrix $\mathcal{O}$ is equal to n, the system is observable. Rigorous observability proofs for nonlinear systems are beyond the scope of this thesis. However, the amount of redundant measurements that can be found in a microgrid means that the observability requirement is easily satisfied in every numerical experiment used to validate the proposed protection scheme.

If the execution of DSE on the updated subset of measurements results in a high confidence level, it can be concluded that the first hypothesis is verified, namely that the instrumentation channel is streaming erroneous measurements and is possibly compromised.

Under a legacy protection scheme, such a situation could trigger tripping decisions and disconnections of legitimate loads. In this case, the centralized scheme blocks the relay monitoring the individual protection zone from tripping a healthy portion of the microgrid based on erroneous measurements. Therefore, the normal operation of a microgrid can be maintained, while its operators are simultaneously alerted about the potential intrusion.

On the other hand, if the confidence level remains low after the DSE execution on the updated measurement set, the proposed scheme returns to the original set of measurements and creates a new updated set by removing only those corresponding to the same protection zone as the suspect measurement. The overall microgrid measurement model is also modified by removing all of its components that correspond to the individual device or devices located within the suspect protection zone. Afterwards, DSE is performed again using both the new updated measurement set, and the new reduced microgrid measurement model.

A high confidence level at this stage would mean that the measurements recorded at the rest of the microgrid fit the model for the rest of the microgrid well. This would indicate that a fault has changed the actual system model as far as the affected zone is concerned, thus creating the mismatch that caused the initial confidence level drop. Therefore, the proposed protection scheme allows the relay monitoring the individual protection zone to trip the breakers. This hypothesis corresponds to a protection system operation similar to legacy protection schemes, but with the additional benefit of adding more confidence to the protection operations.

However, if the second hypothesis cannot be validated, i.e., the DSE at the previous step outputs a low confidence level again, a final hypothesis is studied, namely that there may be a case of a power fault happening simultaneously with the recording of erroneous measurements.

In order to test this hypothesis, the reduced measurement set of the second hypothesis is updated by further removing all measurements recorded from the same instrumentation channel that recorded the suspect measurement. Moreover, the same reduced microgrid measurement model produced during the examination of the second hypothesis is updated by removing all measurement equations corresponding to the newly removed measurements. This processing leads to a new updated measurement set comprising all original measurements that are recorded neither within the suspect protection zone nor from the suspect measurement channel, as well as a corresponding updated microgrid measurement model. Then, the DSE process is executed again. If the resulting confidence level is high, the relay monitoring the individual protection zone is allowed to trip due to the existence of a fault in the system.

Finally, if all three hypotheses are rejected, the hypothesis testing for the selected suspect measurement is considered inconclusive. In that case, the measurement with the next largest absolute normalized residual is chosen as the next suspect measurement, and the hypothesis testing process is executed again. This part of the proposed protection scheme relies on the list of measurements in descending order of absolute normalized residual that has already been created.

The hypothesis testing part of the presented protection scheme reinforces the importance of modularity in the overall design. Specifically, the DSE module may have to be executed up to three additional times for every DSE execution that results in a confidence level drop, under the additional assumption that the first suspect measurement will prove conclusive. Therefore, an independent DSE module is necessary in order to automate the computations for different microgrid measurement models and measurement sets. A modular modeling approach is also of paramount importance, as it may be required to alter the microgrid measurement model during the execution of hypothesis testing, in order to create the alternative models used to test each hypothesis. An object-oriented approach that satisfies these prerequisites is presented in the next chapters.

3.3 Summary

In this chapter, a general explanation of the proposed protection scheme was offered. At its core lies a DSE module which utilizes microgrid measurements in phasor form to estimate the microgrid state and evaluate the consistency of recorded measurements with the model of the microgrid. Discrepancies between measurements and model can be caused by both cyber-attacks and legitimate power faults within the microgrid. Therefore, a hypothesis testing module that can identify the cause of such discrepancies was also introduced. This module relies on additional executions of DSE, which emphasizes the need for modular implementation of the proposed scheme. In the following chapters, each part of the protection algorithm introduced here will be analyzed in more detail.

CHAPTER 4
MICROGRID DEVICE MODELING

High-fidelity microgrid models are necessary for the successful operation of the algorithm described in the previous chapter. Moreover, such models should be modular in order to accommodate the changes in topology caused by the switching on and off of sources and loads during the regular operation of a microgrid. The microgrid model should be quickly formed based only on knowledge of which devices are currently connected and the mathematical model of each device. In this chapter, an object-oriented approach that satisfies these conditions is presented [59, 60, 61, 62, 63].

4.1 Overview

The device modeling procedure begins with the mathematical description of the physical operation of a device in terms of state and control variables. This general mathematical model is called compact device model. A model in this form may contain both equations and inequalities in analytic form, as well as derivative terms of any order. Moreover, there are no linearity requirements for this type of model.

While a compact device model can provide a high-fidelity physical description of device operations, it may not satisfy modularity and tractability requirements. In order to alleviate such problems, the process of quadratization of the compact device model is introduced.

This step guarantees that the model will contain only polynomial terms that are at most quadratic, as well as derivative terms that are at most first order, combined using only addition and subtraction. In order to achieve such goals, the introduction of extra state variables to the model is frequently needed. This type of mathematical model has been named State and Control Quadratized Device Model (SCQDM).

The protection scheme presented in this dissertation utilizes the State and Control Algebraic Quadratic Companion Form (SCAQCF). A mathematical model in SCAQCF is produced by integrating the SCQDM equations to eliminate all existing derivative terms. In this work, the quadratic integration is used, which is an implicit, one-step, A-stable Runge-Kutta method [64, 65, 66].

By eliminating both the differential terms and the nonlinear terms of order higher than two, the computational burden of executing the presented protection algorithm is significantly reduced. The steps of the procedure are shown in Figure 4.1.

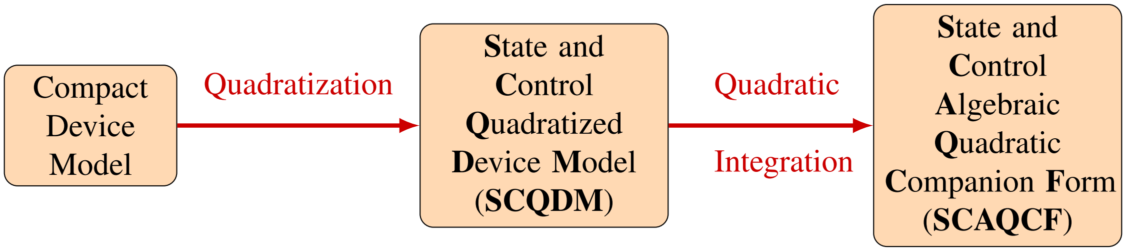
Compact Device Model
Quadratization
State and Control Quadratized Device Model (SCQDM)
Quadratic Integration
State and Control Algebraic Quadratic Companion Form (SCAQCF)

Figure 4.1: Overview of the device modeling procedure.

4.2 Quadratization

The process of converting every analytic term of the compact device model equations into a polynomial of degree at most two is called quadratization. An example of this procedure is the conversion of an arbitrary polynomial into an at most quadratic polynomial.

Assume that

$$y(t) = x^n(t), n \in \mathbb{N}^*. \tag{4.1}$$

Here, the quadratization can be achieved with the following recursive algorithm.

- For $n = 1$ or $n = 2$, the quadratization procedure is successfully terminated.

- For $n = 2^k$ for some integer $k > 1$, additional variables $y_1, \ldots, y_k$ are introduced during the quadratization process in the following way

$$y_1(t) = x^2(t), \tag{4.2}$$

$$y_2(t) = y_1^2(t), \tag{4.3}$$

$$\vdots$$

$$y_k(t) = y_{k-1}^2(t), \tag{4.4}$$

which successfully terminates the quadratization procedure. A simple way to verify whether the exponent n is a power of two is to convert it to its binary representation. In that case, the binary representation will be of the form $10...0$ for some number of trailing zeros.

- For any other $n \in \mathbb{N}^*$, let

$$m = \lfloor \log_2 n \rfloor, \tag{4.5}$$

$$p(t) = x^{2^m}(t), \tag{4.6}$$

$$q(t) = x^{n-2^m}(t). \tag{4.7}$$

Then, $y(t)$ can be written as a product of the two new variables $p(t)$ and $q(t)$ as follows.

$$y(t) = p(t)q(t), \tag{4.8}$$

where $p(t)$ can be further simplified since its exponent is a power of two. Then, the procedure described in this section is repeated recursively for $q(t)$ until one of the terminating conditions is reached.

4.3 State and Control Quadratized Device Model (SCQDM)

The derivation of the SCQDM equations and inequalities is an intermediate step in the device modeling approach. The general syntax of a model in SCQDM is the following.

$$\tilde{\mathbf{I}}(t) = Y_{\text{eqx1}}\tilde{\mathbf{x}}(t) + Y_{\text{equ1}}\tilde{\mathbf{u}}(t) + D_{\text{eqxd1}}\frac{d\tilde{\mathbf{x}}}{dt}(t) + \mathbf{C}_{\text{eqc1}}, \tag{4.9}$$

$$\mathbf{0} = Y_{\text{eqx2}}\tilde{\mathbf{x}}(t) + Y_{\text{equ2}}\tilde{\mathbf{u}}(t) + D_{\text{eqxd2}}\frac{d\tilde{\mathbf{x}}}{dt}(t) + \mathbf{C}_{\text{eqc2}}, \tag{4.10}$$

$$\begin{aligned}\mathbf{0} = {} & Y_{\text{eqx3}}\tilde{\mathbf{x}}(t) + Y_{\text{equ3}}\tilde{\mathbf{u}}(t) + \left\{\begin{matrix}\vdots \\ \tilde{\mathbf{x}}(t)^{\top} F^{i}_{\text{eqxx3}}\tilde{\mathbf{x}}(t) \\ \vdots\end{matrix}\right\} \\ & + \left\{\begin{matrix}\vdots \\ \tilde{\mathbf{u}}(t)^{\top} F^{i}_{\text{equu3}}\tilde{\mathbf{u}}(t) \\ \vdots\end{matrix}\right\} + \left\{\begin{matrix}\vdots \\ \tilde{\mathbf{u}}(t)^{\top} F^{i}_{\text{equx3}}\tilde{\mathbf{x}}(t) \\ \vdots\end{matrix}\right\} + \mathbf{C}_{\text{eqc3}},\end{aligned} \tag{4.11}$$

$$\begin{aligned}\mathbf{g}\left(\tilde{\mathbf{x}}, \tilde{\mathbf{u}}\right) = {} & Y_{\text{hfeqx}}\tilde{\mathbf{x}}(t) + Y_{\text{hfequ}}\tilde{\mathbf{u}}(t) + \left\{\begin{matrix}\vdots \\ \tilde{\mathbf{x}}(t)^{\top} F^{i}_{\text{hfeqxx}}\tilde{\mathbf{x}}(t) \\ \vdots\end{matrix}\right\} \\ & + \left\{\begin{matrix}\vdots \\ \tilde{\mathbf{u}}(t)^{\top} F^{i}_{\text{hfequu}}\tilde{\mathbf{u}}(t) \\ \vdots\end{matrix}\right\} + \left\{\begin{matrix}\vdots \\ \tilde{\mathbf{u}}(t)^{\top} F^{i}_{\text{hfequx}}\tilde{\mathbf{x}}(t) \\ \vdots\end{matrix}\right\} + \mathbf{C}_{\text{hfeqc}},\end{aligned} \tag{4.12}$$

$$\text{subject to} \quad \mathbf{g}\left(\tilde{\mathbf{x}}, \tilde{\mathbf{u}}\right) \leq \mathbf{0}, \tag{4.13}$$

$$\tilde{\mathbf{u}}_{\text{hmin}} \leq \tilde{\mathbf{u}}(t) \leq \tilde{\mathbf{u}}_{\text{hmax}}, \tag{4.14}$$

$$\tilde{\mathbf{x}}_{\text{hmin}} \leq \tilde{\mathbf{x}}(t) \leq \tilde{\mathbf{x}}_{\text{hmax}}. \tag{4.15}$$

Here, $\tilde{\mathbf{I}}$ denotes the terminal through variable vector, $\tilde{\mathbf{x}}$ is the state variable vector, $\tilde{\mathbf{u}}$ represents the control variable vector, $\tilde{\mathbf{x}}_{\text{hmin}}$, $\tilde{\mathbf{x}}_{\text{hmax}}$, $\tilde{\mathbf{u}}_{\text{hmin}}$, $\tilde{\mathbf{u}}_{\text{hmax}}$ are appropriate limits on state and control variables, g is the constraint vector function, Y_{eqx1}, Y_{eqx2}, Y_{eqx3}, Y_{hfeqx} are coefficient matrices for state variables, Y_{equ1}, Y_{equ2}, Y_{equ3}, Y_{hfequ} are coefficient matrices for control variables, D_{eqxd1}, D_{eqxd2} are coefficient matrices for first-order derivatives of state variables, F_{eqxx3}, F_{equu3}, F_{equx3}, $F_{\mathrm{hfeqxx}}, F_{\mathrm{hfequu}}, F_{\mathrm{hfequx}}$ are coefficient matrices for quadratic terms, and $\mathbf{C}_{\mathrm{eqc1}}$, $\mathbf{C}_{\mathrm{eqc2}}$, $\mathbf{C}_{\mathrm{eqc3}}$, $\mathbf{C}_{\mathrm{hfeqc}}$ are appropriate constant vectors.

The SCQDM equations can be split into three groups, namely a) linear through equations (Equation (4.9)), b) linear virtual equations (Equation (4.10)), and c) quadratic virtual equations (Equation (4.11)). The first set contains the equations relating the device through variables to the device state and control variables. Through variables are used to describe currents entering the device through its interface nodes, and for devices that contain only electrical parts this is the sole purpose of the $\tilde{\mathbf{I}}$ vector. The second set relates state and control variables to each other. These equations usually describe the internal state of the device. The third set is similar to the second one, but its equations contain only linear and quadratic terms. Finally, it should also be noted that any of the equation sets described by Equations (4.9) to (4.15) can be left empty.

4.4 Quadratic integration

The quadratic integration is an implicit, one-step, A-stable Runge-Kutta method [64, 65, 66]. In this work, quadratic integration is used to convert the SCQDM model equations to SCAQCF form.

While the trapezoidal method is a popular numerical integration technique for software implementations, it may exhibit oscillatory behavior. This risk is particularly relevant for power system simulations that contain switching devices, most commonly power electronics. The quadratic integration method is preferred in order to avoid such numerical oscillations. Moreover, the quadratic integration method exhibits superior accuracy to the trapezoidal method, as it is 4th-order accurate, while the trapezoidal method is 2nd-order accurate.

According to the trapezoidal method, the function is assumed to vary linearly between two measurements. Instead, the quadratic integration method utilizes an extra measurement at the midpoint of the integration interval, and fits a quadratic polynomial using all three available measurements. A comparison of the trapezoidal and quadratic integration methods is provided in Figure 4.2.

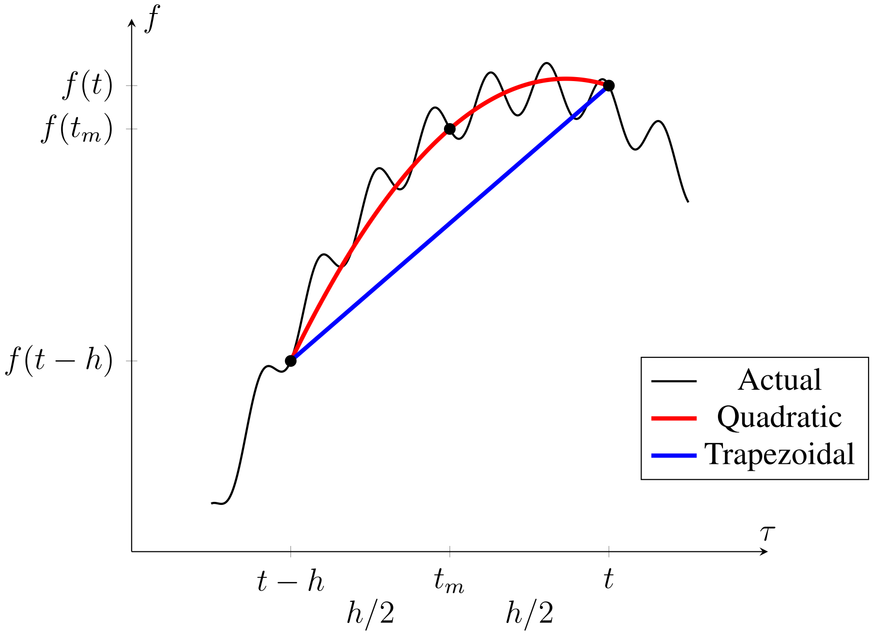

Figure 4.2: Graphic comparison of trapezoidal and quadratic integration methods.

In summary, the quadratic integration method demonstrates superior accuracy, numerical stability, and convergence properties, which are important for power system applications.

4.5 State and Control Algebraic Quadratic Companion Form (SCAQCF)

A model in SCAQCF is the final outcome of the modeling process for an individual device. The conversion step from SCQDM to SCAQCF is executed by quadratically integrating the linear through (Equation (4.9)) and linear virtual (Equation (4.10)) SCQDM equations to eliminate all existing derivative terms, and then affixing the quadratic equations (Equation (4.11)) without further processing.

By eliminating both the nonpolynomial terms and the polynomial terms of order higher than two through quadratization, as well as the differential terms through quadratic integration, the modularity and tractability requirements of the microgrid protection algorithm are satisfied.

The general syntax of a model in SCAQCF is the following.

$$\left\{\begin{matrix}\tilde{\mathbf{I}}(t)\\ \mathbf{0}\\ \mathbf{0}\\ \tilde{\mathbf{I}}(t_m)\\ \mathbf{0}\\ \mathbf{0}\end{matrix}\right\} = Y_{\text{eqx}}\tilde{\mathbf{x}}(t) + Y_{\text{equ}}\tilde{\mathbf{u}}(t) + \left\{\begin{matrix}\vdots\\ \tilde{\mathbf{x}}(t)^{\top}F^{i}_{\text{eqxx}}\tilde{\mathbf{x}}(t)\\ \vdots\end{matrix}\right\}$$

$$+\left\{\begin{matrix}\vdots\\ \tilde{\mathbf{u}}(t)^{\top}F^{i}_{\text{equu}}\tilde{\mathbf{u}}(t)\\ \vdots\end{matrix}\right\} + \left\{\begin{matrix}\vdots\\ \tilde{\mathbf{u}}(t)^{\top}F^{i}_{\text{equx}}\tilde{\mathbf{x}}(t)\\ \vdots\end{matrix}\right\} - \mathbf{B}_{\text{eq}}, \tag{4.16}$$

$$\mathbf{B}_{\text{eq}} = -N_{\text{eqx}}\tilde{\mathbf{x}}(t-h) - N_{\text{equ}}\tilde{\mathbf{u}}(t-h) - M_{\text{eq}}\tilde{\mathbf{I}}(t-h) - \mathbf{K}_{\text{eq}}, \tag{4.17}$$

$$\mathbf{g}\left(\tilde{\mathbf{x}},\tilde{\mathbf{u}}\right) = Y_{\text{feqx}}\tilde{\mathbf{x}}(t) + Y_{\text{fequ}}\tilde{\mathbf{u}}(t) + \left\{\begin{matrix}\vdots\\ \tilde{\mathbf{x}}(t)^{\top}F^{i}_{\text{feqxx}}\tilde{\mathbf{x}}(t)\\ \vdots\end{matrix}\right\}$$

$$+\left\{\begin{matrix}\vdots\\ \tilde{\mathbf{u}}(t)^{\top}F^{i}_{\text{fequu}}\tilde{\mathbf{u}}(t)\\ \vdots\end{matrix}\right\} + \left\{\begin{matrix}\vdots\\ \tilde{\mathbf{u}}(t)^{\top}F^{i}_{\text{fequx}}\tilde{\mathbf{x}}(t)\\ \vdots\end{matrix}\right\} + \mathbf{C}_{\text{feqc}}, \tag{4.18}$$

$$\text{subject to}\quad \mathbf{g}\left(\tilde{\mathbf{x}},\tilde{\mathbf{u}}\right) \leq \mathbf{0}, \tag{4.19}$$

$$\tilde{\mathbf{u}}_{\text{min}} \leq \tilde{\mathbf{u}}(t) \leq \tilde{\mathbf{u}}_{\text{max}}, \tag{4.20}$$

$$\tilde{\mathbf{x}}_{\text{min}} \leq \tilde{\mathbf{x}}(t) \leq \tilde{\mathbf{x}}_{\text{max}}. \tag{4.21}$$

For Equations (4.16) to (4.21), $\tilde{\mathbf{I}}$ denotes the terminal through variable vector, $\tilde{\mathbf{x}}$ is the state variable vector, $\tilde{\mathbf{u}}$ represents the control variable vector, $\tilde{\mathbf{x}}_{\mathrm{min}}$, $\tilde{\mathbf{x}}_{\mathrm{max}}$, $\tilde{\mathbf{u}}_{\mathrm{min}}$, $\tilde{\mathbf{u}}_{\mathrm{max}}$ are appropriate limits on state and control variables, $\mathbf{g}$ is the constraint vector function, Y_{eqx}, N_{eqx}, Y_{feqx} are coefficient matrices for state variables, Y_{equ}, N_{equ}, Y_{fequ} are coefficient matrices for control variables, F_{eqxx}, F_{equu}, F_{equx}, F_{feqxx}, F_{fequu}, F_{fequx} are coefficient matrices for quadratic terms, M_{eq} is a coefficient matrix for through variables, and $\mathbf{K}_{\mathrm{eq}}$, $\mathbf{C}_{\mathrm{feqc}}$ are appropriate constant vectors, h is the integration step, and t_m is the midpoint of the integration interval.

As the system of equations represented by Equation (4.16) is derived from corresponding SCQDM equations (Equations (4.9) to (4.11)), its components maintain the categorization into a) linear through equations, b) linear virtual equations, and c) quadratic virtual equations.

4.6 Summary

In this chapter, an object-oriented modeling approach was introduced in order to enable the fast operation of the proposed protection scheme. This approach relies on three different types of models, namely compact device models, SCQDM, and models in SCAQCF. Any arbitrary equation that describes physical properties of a power device can be cast in any of these three models with appropriate manipulations, if necessary. Therefore, the intermediate conversion steps between these three equivalent representations are also presented. The end product is the SCAQCF, which is suitable for physically based, high fidelity models that can offer the necessary modularity and tractability for the operation of the novel protection scheme. Table 4.1 summarizes the main characteristics of the three model types.

Table 4.1: Summary of model types

Type	Suitable equations	Derivative terms	Non-derivative terms
Compact	Any physical device equation	Any derivative term	Any analytic term
SCQDM	Any physical device equation	Only up to first order derivatives	Only polynomials up to second order
SCAQCF	Any physical device equation	No derivative terms	Only polynomials up to second order

CHAPTER 5
MICROGRID MEASUREMENT MODELING

The individual device modeling procedure placed great emphasis on modularity, as the topology of a microgrid may undergo frequent changes. In this chapter, a procedure is introduced that aims to form an SCAQCF model for the full microgrid by combining its component device SCAQCF models. Subsequently, an appropriate model for the microgrid measurements is extracted from the microgrid SCAQCF model.

5.1 Overview

The SCAQCF syntax offers a common framework that can describe individual components, combinations of components, and even a whole microgrid. By unifying parts of the grid of any size under the same rules, the applied protection logic can be greatly simplified.

A microgrid-level SCAQCF model may have some interface nodes with other interconnected systems. The device-level linear through SCAQCF equations corresponding to such nodes are added to the set of microgrid-level linear through SCAQCF equations after mapping the device-level state and control variables onto microgrid-level state and control variables. Then, for each internal microgrid node, the device-level linear through SCAQCF equations corresponding to devices connected to that node are summed to form a new equation according to Kirchhoff's Current Law (KCL). At this step, device-level through variables are eliminated and device-level state and control variables are replaced with microgrid-level state and control variables. Finally, the device-level linear virtual and quadratic virtual equations for each device are appended to the respective sets of microgrid-level equations after the mapping of device-level state and control variables onto microgrid-level state and control variables. This procedure is shown in Figure 5.1.

As the SCAQCF modeling paradigm is very flexible, non-electrical (e.g., mechanical)

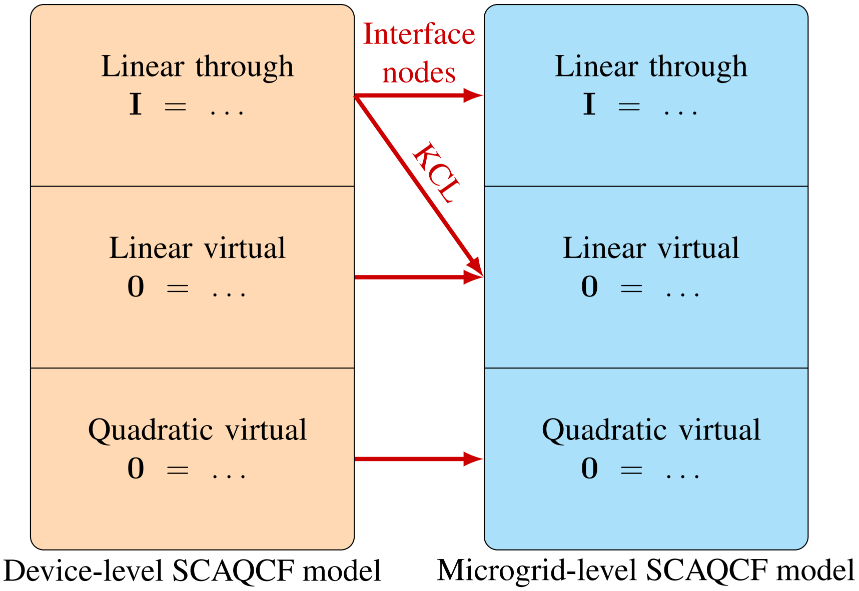

Figure 5.1: Overview of the microgrid-level SCAQCF model derivation.

linear through equations may also exist. In that case physical laws analogous to KCL (e.g., Newton's Laws) can be applied at the interface of such non-electrical system parts.

Once a microgrid-level SCAQCF model is obtained, the microgrid measurement model that is necessary for the presented protection approach can be extracted. The microgrid measurement model is described by a vector function denoted as $\mathbf{h}(\tilde{\mathbf{x}}, \tilde{\mathbf{u}})$, and it should describe at least all quantities measured by measurement units installed in the actual microgrid. This is feasible, because all measured quantities are part of the microgrid-level SCAQCF model. Moreover, since measurement redundancy is important for the proper operation of this protection scheme, microgrid-level SCAQCF equations can be appropriately manipulated to offer extra measurement equations.

5.2 Microgrid SCAQCF model formulation

A device SCAQCF model is organized as shown in Equations (4.16) to (4.21). In Equation (4.16), the vector components corresponding to $\tilde{\mathbf{I}}$ terms are called linear through equations, and they describe the way an SCAQCF model may interact with adjacent SCAQCF models. When these equations are considered alongside information on the interconnections between devices, individual SCAQCF models can be combined into a larger SCAQCF model.

For example, for a purely electrical device, linear through equations would describe currents flowing into the device from each of its interface terminals. For a microgrid that contains such devices, knowledge of its topology would reveal which device terminals are connected to each microgrid node. Moreover, microgrid nodes can be split into a) nodes at the interface of the microgrid with the rest of the power grid, and b) internal microgrid nodes. When a device interface terminal is also a microgrid interface terminal, no processing of the corresponding linear through equation is needed. However, for a given internal microgrid node, KCL should be applied to sum all the linear through equations corresponding to currents flowing into the device terminals that are connected to that node. This will create a new equation with a zero on its left-hand side, which means that it will belong to the set of linear virtual equations of the resulting SCAQCF model. Therefore, the device-level sets of linear through equations can be used to generate the microgrid-level set of linear through equations, as well as part of the microgrid-level set of linear virtual equations. The device-level sets of virtual equations, both linear and quadratic, are then appended to the microgrid-level sets of equations of the same name.

During this procedure, it is important to maintain a mapping between the device-level states, and the microgrid-level states. In the above example, the device-level terminal voltages should be device-level state variables, which are then linked to the corresponding microgrid-level nodal voltage state variable.

An example of this procedure can be found in Figure 5.2. Node α is a microgrid interface node. Therefore, the linear through SCAQCF equation for $i_{A,1}$, which is a device A equation, becomes a linear through equation for the microgrid SCAQCF model. The only prerequisite for this is the substitution of device-level state and control variables for device A with microgrid-level equivalents. On the other hand, node β is an internal microgrid node. There are four device terminals connected to β, each with a corresponding linear through equation for the terminal current. KCL is then used to sum these four linear through equations, i.e., $0 = i_{A,2} + i_{B,1} + i_{C,1} + i_{D,1}$. As this equation has a zero on its left-hand side, the result becomes part of the linear virtual equation set of the microgrid-level SCAQCF model. All four currents on the right-hand side of the equation are replaced with the corresponding device-level SCAQCF expressions that are functions of the device-level state and control variables. The final step of this procedure is the replacement of device-level state and control variables for devices A, B, C and D with appropriate microgrid-level state and control variables.

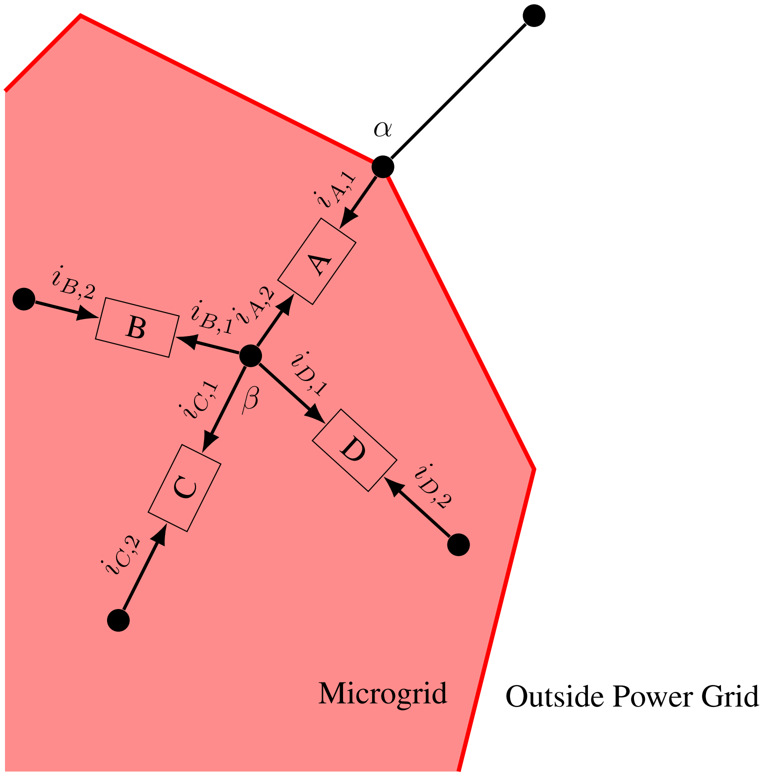

Figure 5.2: Microgrid-level SCAQCF model derivation example. The $i_{A,1}$ device-level linear through equation is retained for the microgrid-level SCAQCF model. The $i_{A,2}$, $i_{B,1}$, $i_{C,1}$, $i_{D,1}$ equations are combined through KCL to form a microgrid-level SCAQCF linear virtual equation.

The repetition of the procedure of the previous paragraph for all microgrid nodes leads to the processing of all device-level linear through SCAQCF equations. Finally, device-level virtual SCAQCF equations are appended to the corresponding microgrid-level SCAQCF equation sets after appropriate mappings between device-level and microgrid-level variables.

Thus, individual devices can be combined in a systematic way to form models for larger groups, such as microgrids.

5.3 Measurement model formulation

Once a microgrid-level SCAQCF model is obtained, the process to extract a model for the microgrid measurements can start. The measurement model is denoted as $\mathbf{h}(\tilde{\mathbf{x}}, \tilde{\mathbf{u}})$, and its measurements can be categorized into a) actual measurements, b) derived measurements, c) virtual measurements, and d) pseudo measurements.

The first step is the formation of the actual measurement portion of the microgrid measurement model. It should be noted that these are the equations corresponding to real measurements received from the installed measuring instruments. The procedure described in the previous paragraph also offers as a byproduct a mapping of device-level variables and equations to microgrid-level variables and equations. This mapping is useful for the formation of the actual measurement portion of the microgrid measurement model.

Actual measurements can be further split into a) across actual measurements, and b) through actual measurements.

Measurements of the first category are only functions of state variables. They can be defined either at the microgrid level directly or at any intermediate level including the individual device level. The latter case is possible due to the variable mappings that have already been obtained while forming the microgrid-level SCAQCF model. Specifically, an across measurement can be described by the following equation.

$$\tilde{\mathbf{z}}(t) = A\tilde{\mathbf{x}}(t) + \boldsymbol{\eta} \tag{5.1}$$

where $\tilde{\mathbf{z}}$ denotes the measurement vector, A is the coefficient matrix for state variables, and

$\boldsymbol{\eta}$ is the error term vector. Equivalently, an across actual measurement equation is a linear combination of states.

In contrast, through actual measurements are usually better defined at the individual device level. The reason for this is that their measurement equations are derived from SCAQCF linear through equations. Every microgrid-level SCAQCF linear through equation is also a device-level equation, but the opposite is generally not true.

A through actual measurement at the device-level can be described by the following equations.

$$\tilde{\mathbf{z}}(t) = Y_{\text{fzx}}\tilde{\mathbf{x}}(t) + Y_{\text{fzu}}\tilde{\mathbf{u}}(t) + \left\{ \begin{matrix} \vdots \\ \tilde{\mathbf{x}}(t)^\top F^i_{\text{fzxx}}\tilde{\mathbf{x}}(t) \\ \vdots \end{matrix} \right\}$$
$$+ \left\{ \begin{matrix} \vdots \\ \tilde{\mathbf{u}}(t)^\top F^i_{\text{fzuu}}\tilde{\mathbf{u}}(t) \\ \vdots \end{matrix} \right\} + \left\{ \begin{matrix} \vdots \\ \tilde{\mathbf{u}}(t)^\top F^i_{\text{fzux}}\tilde{\mathbf{x}}(t) \\ \vdots \end{matrix} \right\} - \mathbf{B}_{\text{fz}} + \boldsymbol{\eta}, \qquad (5.2)$$

$$\mathbf{B}_{\text{fz}} = -N_{\text{fzx}}\tilde{\mathbf{x}}(t-h) - N_{\text{fzu}}\tilde{\mathbf{u}}(t-h) - M_{\text{fz}}\tilde{\mathbf{I}}(t-h) - \mathbf{K}_{\text{fz}}. \qquad (5.3)$$

Here, $\tilde{\mathbf{z}}$ denotes the measurement vector, $\tilde{\mathbf{I}}$ is the terminal through variable vector, $\tilde{\mathbf{x}}$ denotes the state variable vector, $\tilde{\mathbf{u}}$ represents the control variable vector, Y_{fzx}, N_{fzx} are coefficient matrices for state variables, Y_{fzu}, N_{fzu} are coefficient matrices for control variables, F_{fzxx}, F_{fzuu}, F_{fzux} are coefficient matrices for quadratic terms, M_{fz} is a coefficient matrix for through variables, $\mathbf{K}_{\text{fz}}$ is an appropriate constant vector, h is the integration step, and $\boldsymbol{\eta}$ is the error term vector.

Derived measurements are obtained using recorded values for actual measurements and knowledge of the microgrid topology. The simplest example for this procedure is a current measurement on a device terminal connected to a node where only one other device terminal is attached. Due to KCL, the currents going into each terminal have the same magnitude and opposite direction, so measuring one of them offers not only an actual measurement for the terminal with the attached measuring device, but also a derived measurement for the other terminal. This the case with the actual measurement for i_x and the derived measurement for i_y in Figure 5.3. Moreover, an actual measurement for v_x can provide a derived measurement for v_y due to Kirchhoff's Voltage Law (KVL).

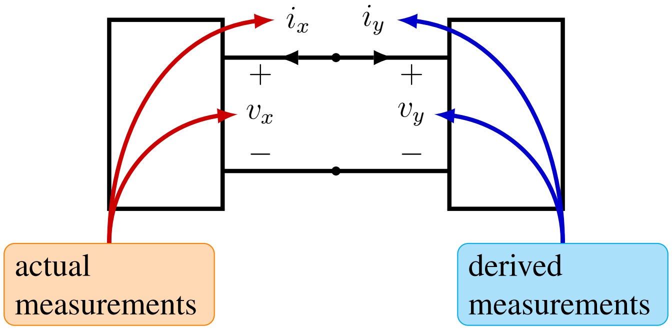

Figure 5.3: Derived measurements example.

During the formation of the microgrid-level SCAQCF model, all equations produced through the application of KCL on current equations of individual devices, as well as all equations obtained from linear virtual and quadratic equations of individual devices, will have zeros on their left-hand sides. These zeros can also be treated as measurements, which are called virtual. This is possible because each of these zeros can be treated as a function of the state and control variables on the other side of the equation, which happens to equal zero for any time t.

Finally, there are quantities that are not measured normally, and for which approximate values are known (e.g., the voltage of neutral conductors is normally close to zero). Such quantities can be included as pseudo measurements.

Thus, the general form of the measurement SCAQCF model is described by the following equations.

$$\tilde{\mathbf{z}}(t) = Y_{\mathrm{zx}}\tilde{\mathbf{x}}(t) + Y_{\mathrm{zu}}\tilde{\mathbf{u}}(t) + \left\{\begin{array}{c} \vdots \\ \tilde{\mathbf{x}}(t)^\top F^i_{\mathrm{zxx}}\tilde{\mathbf{x}}(t) \\ \vdots \end{array}\right\}$$

$$+ \left\{\begin{array}{c} \vdots \\ \tilde{\mathbf{u}}(t)^\top F^i_{\mathrm{zuu}}\tilde{\mathbf{u}}(t) \\ \vdots \end{array}\right\} + \left\{\begin{array}{c} \vdots \\ \tilde{\mathbf{u}}(t)^\top F^i_{\mathrm{zux}}\tilde{\mathbf{x}}(t) \\ \vdots \end{array}\right\} - \mathbf{B}_{\mathrm{z}} + \boldsymbol{\eta}, \tag{5.4}$$

$$\mathbf{B}_{\mathrm{z}} = -N_{\mathrm{zx}}\tilde{\mathbf{x}}(t-h) - N_{\mathrm{zu}}\tilde{\mathbf{u}}(t-h) - M_{\mathrm{z}}\tilde{\mathbf{I}}(t-h) - \mathbf{K}_{\mathrm{z}}. \tag{5.5}$$

In the equations above, $\tilde{\mathbf{z}}$ denotes the measurement vector, $\tilde{\mathbf{I}}$ is the terminal through variable vector, $\tilde{\mathbf{x}}$ denotes the state variable vector, $\tilde{\mathbf{u}}$ represents the control variable vector, Y_{zx}, N_{zx} are coefficient matrices for state variables, Y_{zu}, N_{zu} are coefficient matrices for control variables, F_{zxx}, F_{zuu}, F_{zux} are coefficient matrices for quadratic terms, M_{z} is a coefficient matrix for through variables, $\mathbf{K}_{\mathrm{z}}$ is an appropriate constant vector, h is the integration step, and $\boldsymbol{\eta}$ is the error term vector.

It is evident that error terms for different categories of measurements cannot be identical, as the value of a virtual measurement is certain (and equal to zero), while the value of a pseudo measurement is essentially the result of a guess. In order to handle this, different standard deviations of the measurement error are assigned to different types of measurements. Specifically, actual and, thus, derived measurements are assigned the standard deviation of the corresponding measuring device, virtual measurement error is assigned a very low standard deviation, and pseudo measurement error is assigned a very high standard deviation. Assuming a microgrid where all measuring instruments have standard deviations of the same order of magnitude, a good choice would be to assign to virtual measurements a standard deviation two orders of magnitude smaller, and to pseudo measurements a standard deviation two orders of magnitude larger, than the standard deviation for actual measurements.

5.4 Summary

This section introduced a procedure to combine individual device SCAQCF models into an SCAQCF model that describes a whole microgrid. Then, it explained how to use the microgrid SCAQCF model to extract a microgrid measurement model. Such a model may contain four types of measurements, namely actual, derived, virtual, and pseudo measurements. Finally, this section concluded with a discussion about measurement error terms, which will be useful for Chapter 6.

CHAPTER 6

DYNAMIC STATE ESTIMATION AND HYPOTHESIS TESTING

The analysis of microgrid data for fault and cyber-attack identification relies on the accurate estimation of the microgrid state through DSE. Alongside the measurements that are being continuously streamed by microgrid measurement devices, the derivation of a high-fidelity microgrid measurement model according to the process described in the previous chapter is a prerequisite for the efficient operation of this algorithm. This chapter presents the techniques for microgrid state estimation and assessment, and also offers a comprehensive analysis of the hypothesis testing mechanism.

6.1 Weighted Least Squares (WLS)

The presented protection scheme relies heavily on the execution of DSE through the WLS method. At every instant that DSE is used to estimate the system state, an optimization problem is solved. Specifically, let $J(\tilde{\mathbf{x}}, \tilde{\mathbf{u}})$ be the objective function given by

$$\begin{aligned} J(\tilde{\mathbf{x}}, \tilde{\mathbf{u}}) &= \left(\mathbf{h}(\tilde{\mathbf{x}}, \tilde{\mathbf{u}}) - \tilde{\mathbf{z}}\right)^\top W \left(\mathbf{h}(\tilde{\mathbf{x}}, \tilde{\mathbf{u}}) - \tilde{\mathbf{z}}\right) \\ &= \sum_{i=1}^{n} \left(\frac{h_i(\tilde{\mathbf{x}}, \tilde{\mathbf{u}}) - \tilde{z}_i}{\sigma_i}\right)^2 . \end{aligned} \tag{6.1}$$

where n is the total number of measurements, z_i is the value of the i-th measurement, h_i is the SCAQCF measurement model equation for the i-th measurement in terms of system state and control variables, σ_i is the standard deviation of the i-th measurement, and the weight matrix W is a diagonal matrix with $W_{ii} = \sigma_i^{-2}$.

The specific values of the control variables at each iteration of the DSE can be substituted in the measurement model equations yielding a function only in terms of the state variables. The optimization problem then is simply

$$\min_{\tilde{\mathbf{x}}} J(\tilde{\mathbf{x}}). \tag{6.2}$$

This nonlinear unconstrained optimization problem can be solved using Newton's method as follows

$$\tilde{\mathbf{x}}^{k+1} = \tilde{\mathbf{x}}^{k} - \left(H^\top W H\right)^{-1} H^\top W \left(\mathbf{h}(\tilde{\mathbf{x}}^{k}) - \tilde{\mathbf{z}}\right), \tag{6.3}$$

where $H = \frac{\partial \mathbf{h}(\tilde{\mathbf{x}}^k)}{\partial \tilde{\mathbf{x}}}$ is the appropriate Jacobian matrix at the k-th iteration. It should be noted that for linear equations, only one iteration of Equation 6.3 is required. The final product of this procedure is an estimated state $\hat{\mathbf{x}}$.

6.2 Estimated measurements and confidence level

The assessment of the operational state of the microgrid is based on the microgrid confidence level. This is a metric for the goodness of fit of the obtained measurements given the microgrid measurement model. The calculation of an estimate $\hat{\mathbf{x}}$ of the microgrid state is a prerequisite for this part of the process.

The estimated measurement $h_i(\hat{\mathbf{x}})$ can be obtained for the i-th measurement, once the estimated microgrid state $\hat{\mathbf{x}}$ is computed. Estimated measurements show the predicted value for a measured physical quantity within the microgrid given a state estimate $\hat{\mathbf{x}}$.

The differences between recorded measurement values and the corresponding estimated measurements are very important, as they may indicate abnormal behavior. Thus, the sum of the squared normalized residuals ζ is calculated as

$$\zeta = \sum_{i=1}^{n} \left(\frac{h_i(\hat{\mathbf{x}}) - \tilde{z}_i}{\sigma_i}\right)^2. \tag{6.4}$$

Finally, the confidence level is simply

$$\begin{aligned}\Pr\left\{\chi^2 \geq \zeta\right\} &= 1 - \Pr\left\{\chi^2 \leq \zeta\right\} \\ &= 1 - F_{\chi^2}(\zeta, \nu),\end{aligned} \tag{6.5}$$

where F_{χ^2} is the cumulative distribution function of the χ^2 distribution, and ν denotes the degrees of freedom.

A substantial drop in the confidence level is used as an abnormality indicator. There is flexibility in defining which confidence level drops are considered substantial. At the very least, a minimum acceptable confidence level should be defined during the deployment of this protection scheme. In order to avoid triggering the protection scheme during momentary spikes, the duration of the drop can be taken into account. One possible way to achieve this is by summing the confidence level over some rolling window.

Specifically, as the process of gathering measurements and executing DSE is periodically repeated at discrete time steps, let $p[t]$ be the confidence level calculated at time step t. Then, the average confidence level at time step t is defined as

$$\bar{P}[t] = \frac{1}{L} \sum_{i=t-L}^{t} p[i]. \tag{6.6}$$

By selecting an appropriate size for the window length L, as well as a minimum threshold for the average confidence level $\bar{P}$, this protection scheme can take momentary spikes into account.

6.3 Hypothesis testing

6.3.1 Normalized residuals

During the introduction of this protection scheme, special emphasis was placed on normalized residuals as indicators of measurements that may have been compromised. The absolute normalized residual r_n corresponding to the i-th measurement is

$$r_{n,i} = \left| \frac{h_i(\hat{\mathbf{x}}) - \tilde{z}_i}{\sigma_i} \right| . \tag{6.7}$$

Normalized residuals are calculated at every DSE iteration. They can essentially be viewed as a byproduct of the calculation of ζ in Equation 6.4. Therefore, the ordering of SCAQCF measurement model equations h_i in descending order of absolute normalized residual $r_{n,i}$ is a process with low computational burden.

6.3.2 Measurement and state variable sets

This subsection describes the ways in which the hypothesis testing process interacts with the microgrid measurement model. Table 6.1 summarizes the possible actions that can be used to manipulate the microgrid-level set of measurement equations in order to create new appropriate measurement sets for different hypotheses.

Table 6.1: Hypothesis testing: Measurement and state removal

Action(s)	Measurement equation h_i	State x_j
Remove by channel	Remove if recorded by the same channel as suspect measurement	Do not remove
Remove by zone	Remove if recorded in the same zone as suspect measurement	Remove if originally from the same zone as suspect measurement
Remove by channel & remove by zone	Remove if recorded either by the same channel or in the same zone as suspect measurement	Remove if originally from the same zone as suspect measurement

Therefore, the cyber-attack hypothesis corresponds to the *Remove by channel* action, the power fault hypothesis to the *Remove by zone* action, and the simultaneous combination of cyber-attack and fault hypothesis to the *Remove by channel & remove by zone* action. Every time a measurement equation h_i is removed, the corresponding measurement $\tilde{z}_i$ must also be eliminated.

There are four measurement categories, namely a) actual measurements, b) derived measurements, c) virtual measurements, and d) pseudo measurements. These are handled differently during hypothesis testing.

Specifically, the *Remove by channel* action will remove every measurement equation h_i corresponding to an actual measurement (whether across or through) recorded by the same instrumentation channel as the suspect measurement. It will also remove any derived measurement equation that is obtained from an actual measurement streamed by the suspect channel. However, this action will not affect any virtual or pseudo measurements. Moreover, it will not eliminate any microgrid-level state.

On the other hand, the *Remove by zone* action will remove every measurement equation h_i associated with the same protection zone as the suspect measurement. This will include every actual through measurement recorded at a terminal of an individual device contained within the suspect protection zone, as well as every actual across measurement that depends on at least one device-level state of a component device of the zone. The same rules apply to pseudo measurements. Derived measurement equations which correspond to physical quantities within the suspect protection zone will be eliminated too, even if they are obtained using an IED in another protection zone. Furthermore, this action will also eliminate every microgrid-level virtual measurement equation originating from a device-level SCAQCF model that describes an individual device within the suspect protection zone. As all relevant measurement equations are removed, no estimate can be obtained for the microgrid-level states that are mapped to device-level states of the zone. Thus, it is also necessary to reduce the set of state variables, when *Remove by zone* is performed.

Finally, the *Remove by channel & remove by zone* action simply combines the other two actions.

The successful execution of the actions of Table 6.1 relies on the accurate labeling of measurement equations by zone and channel. A measurement equation h_i can be better understood as $h_i^{(j,k)}$ with j denoting the j-th protection zone and k indicating the k-th instrumentation channel (usually some specific metering device). An efficient way to codify these relationships is the formation of a *ZoneMeasurements* list for each microgrid protection zone that comprises all measurements associated with that zone, and a *ChannelMeasurements* list for each instrumentation channel that includes all of its measurements.

6.3.3 Redundancy

The hypothesis testing process relies on the elimination of different sets of measurements, which means that a high level of redundancy is required for the proper operation of this protection scheme.

In order to quantify this need, the redundancy coefficient R_c is defined as

$$R_c = \frac{n_z}{n_x}, \tag{6.8}$$

where n_z is the total number of microgrid measurements regardless of type (i.e., it includes actual, derived, virtual, and pseudo measurements), and n_x is the total number of microgrid-level states.

The redundancy requirements of this novel protection scheme can be met by utilizing the metering equipment installed in various microgrids, as well as the additional measurement types (i.e., derived, virtual, pseudo) that can be incorporated into the protection algorithm. Of course, the need for high levels of redundancy does not imply that all actual measurements should be duplicated. For example, the authors in [67] demonstrate that a protection scheme based on DSE can successfully detect a transmission line fault even while losing all current measurements on one side of the line due to communications failure. This example shows that estimation based protection schemes can be designed to be robust to measurement loss or removal.

6.3.4 Illustrative example

In order to further illustrate how hypothesis testing works, it is worth revisiting the example in Figure 5.2 and slightly modifying it. In Figure 6.1, there are four protection zones (A, B, C, and D), and five instrumentation channels (I, II, III, IV, and V). Each protection zone can contain more than one device, and each instrumentation channel can transmit measurements from multiple protection zones. Assume that measurement $i_2^{A,II}$ is suspect. That means that DSE was executed, the confidence level was judged to be low, and $i_2^{A,II}$ has either the largest absolute normalized residual, or all measurements with higher largest absolute normalized residual lead to inconclusive hypothesis testing.

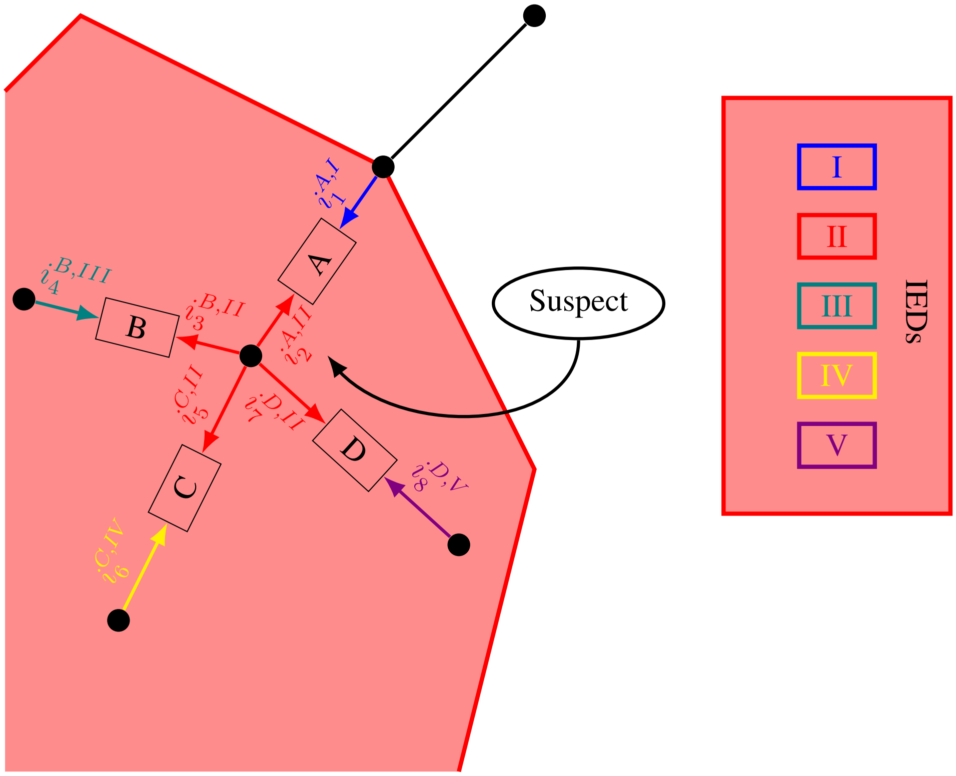

Figure 6.1: Hypothesis testing on a sample microgrid. The introduced centralized protection scheme monitors a microgrid consisting of four protection zones (A, B, C, D) and five IEDs (I, II, III, IV, V).

Cyber-attack hypothesis

For the cyber-attack hypothesis, the *Remove by channel* action is performed. This action will create a new updated measurement set by removing all equations corresponding to IED II, i.e., the actual through measurement equations for $i_2^{A,II}$, $i_3^{B,II}$, $i_5^{C,II}$, and $i_7^{D,II}$. The corresponding measurement values $\tilde{z}_i$ will also be eliminated. No changes will be made to the state variable set. The removal of measurements leads to a lower redundancy level, which stresses the importance of starting with high redundancy. Afterwards, DSE is executed again. If the result is an acceptable confidence level, IED II is considered compromised, the system operator is notified, and the relays monitoring zones A, B, C, and D are prevented from issuing tripping commands.

Power fault hypothesis

If the confidence level of the previous hypothesis remained low, all measurements removed by the previous action are returned to the measurement set. Then, the *Remove by zone* action is performed. This will remove all measurements corresponding to zone A, which includes not only $i_1^{A,I}$ and $i_2^{A,II}$, but also every actual across measurement recorded within the zone, as well as every virtual measurement generated through the zone device models, and every pseudo measurement for quantities inside the zone. Moreover, the relevant values $\tilde{z}_i$ will also be eliminated, and an updated measurement set will be obtained. The state variable set should also be updated by removing all state variables from within protection zone A. This can be easily achieved through the lists mapping the device-level state and control variables onto microgrid-level state and control variables. Then, DSE is repeated. If the output confidence level is restored to an acceptable value, the existence of a power fault is identified as the reason for the mismatches between recorded microgrid measurements and estimated microgrid measurements, so zone A is allowed to trip.

Simultaneous cyber-attack and power fault hypothesis

If none of the previous two hypotheses revealed why the DSE returned a low confidence level, the *Remove by channel & remove by zone* action is executed. This action starts with the measurement and state variable sets obtained through the *Remove by zone* action, and proceeds to also remove all remaining equations corresponding to IED II, namely $i_3^{B,II}$, $i_5^{C,II}$, and $i_7^{D,II}$. Once more, every measurement value $\tilde{z}_i$ corresponding to a removed measurement equation h_i is also removed. Afterwards, DSE is executed again, and a new confidence level is calculated. If it is within acceptable limits, a case of simultaneous cyber-attack and power fault is declared, zone A is allowed to trip to clear the fault, and the microgrid operator is notified about the possible intrusion. However, if the confidence level is again considered low, the suspect measurement $i_2^{A,II}$ is marked as inconclusive. Then, the measurement with the next highest absolute normalized residual is selected as suspect, and the hypothesis testing module starts again.

6.4 Summary

In this section, the DSE problem was formulated as a nonlinear unconstrained optimization problem through the use of WLS. This formulation can be solved through Newton's method and provide an estimate for the microgrid state. Once such an estimate is obtained, both the microgrid confidence level and the measurement normalized residuals can be calculated. The first is a measure for the goodness of fit of the microgrid measurements given the microgrid model, while the latter are intermediate quantities that are useful for hypothesis testing. If a low confidence level is detected, hypothesis testing is necessary to distinguish between power faults and cyber-attacks, and an appropriate algorithm for the hypothesis testing module was provided in this section.

CHAPTER 7

PROTECTION SCHEME DEMONSTRATION

The proposed protection scheme has been extensively tested using microgrid models of various sizes. Two characteristic examples are presented in this chapter. They demonstrate the ability of the introduced protection scheme to successfully detect abnormalities in microgrid operation, as well as identify whether a detected abnormality should be attributed to a cyber-attack, a power fault, or a combination of both. The examples presented in the rest of this chapter also show the flexibility of the underlying modeling approach, which enables the seamless integration of different device models, including high-fidelity models for inverter-interfaced equipment.

7.1 Simplified Microgrid Model

The first example focuses on a microgrid that operates in grid-connected mode and contains a transformer bank consisting of three single-phase transformers. Each transformer is protected as an independent protection zone, and the effect of both a fault and a cyber-attack on these protection zones is examined [68].

7.1.1 Microgrid schematic and description

The schematic of the combination of the microgrid with a simplified equivalent of the larger system is shown in Figure 7.1.

The larger power system contains an equivalent representation for generation and transmission which is connected to the distribution system through a 30 MVA, 115 kV/13.8 kV three-phase transformer in a delta-wye configuration with grounded wye. The distribution system provides service to two 8 MW three-phase loads, as well as a 500 kVA solar power plant and the microgrid under study.

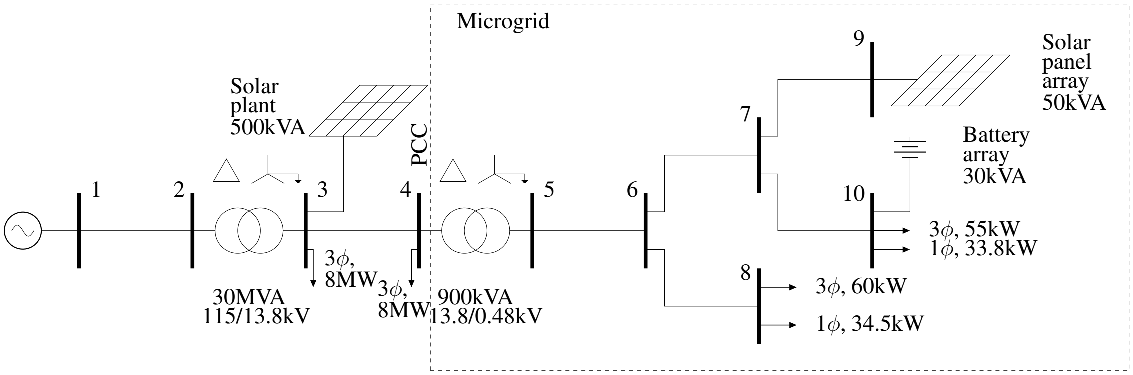

Figure 7.1: Simple test system.

The microgrid is connected to the rest of the power grid at the Point of Common Coupling (PCC) (Bus 4) with a transformer bank consisting of three 300 kVA, 13.8 kV/277 V single-phase transformers in a delta-wye configuration with grounded wye. It contains two three-phase loads and two single-phase loads alongside a 50 kVA three-phase solar panel array and a 30 kVA/5 kWh three-phase battery array. The lengths of the circuits vary between 30 m and 100 m. A summary is provided in Tables 7.1 to 7.2.

Table 7.1: First Microgrid Test System: Distributed Generation

Bus	Type	Nominal Voltage	Nominal Power
9	Solar Panel Array	480 V	50 kVA
10	Battery Array	480 V	30 kVA

Table 7.2: First Microgrid Test System: Load

Bus	Type	Nominal Voltage	Nominal Power
8	3-phase	480 V	55 kW
8	1-phase	480 V	33.8 kW
10	3-phase	480 V	60 kW
10	1-phase	480 V	34.5 kW

7.1.2 Protection zone schematic and description

Each 300 kVA, 13.8 kV/277 V single-phase transformer forms its own protection zone. The three protection zones of the transformer bank are the focus of this study. The schematic for the zone protecting the i-th transformer is shown in Figure 7.2 with marked measurement locations.

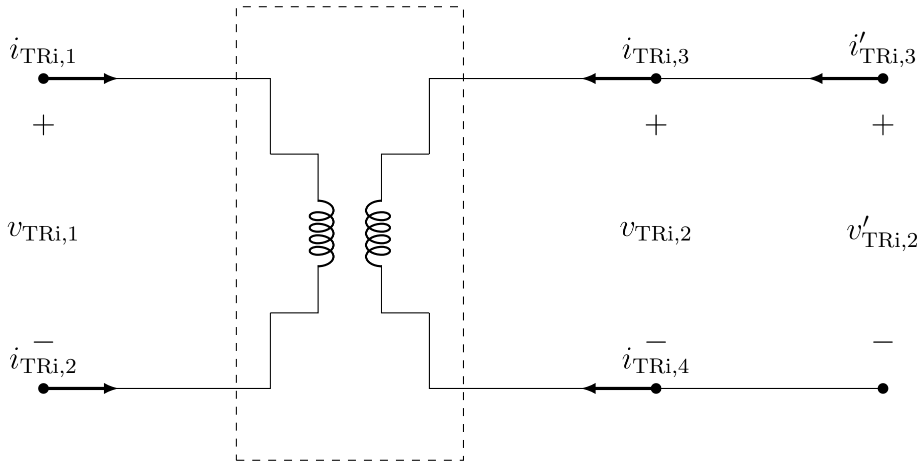

Figure 7.2: Protection zone schematic.

Here, $i_{\mathrm{TRi},1}$, $i_{\mathrm{TRi},2}$, $i_{\mathrm{TRi},3}$, and $i_{\mathrm{TRi},4}$ are actual measurements corresponding to currents flowing into the i-th single-phase transformer TRi taken at the respective transformer, while $i'_{\mathrm{TRi},3}$ is an actual current measurement of the same quantity as $i_{\mathrm{TRi},3}$ but this time recorded at Bus 5. Similarly, $v_{\mathrm{TRi},1}$ and $v_{\mathrm{TRi},2}$ are actual measurements of transformer voltages taken at each transformer, whereas $v'_{\mathrm{TRi},2}$ is an actual voltage measurement at Bus 5.

It is worth stating that actual measurements recorded at Bus 5, namely $i'_{\mathrm{TRi},3}$ and $v'_{\mathrm{TRi},2}$, significantly contribute to the high levels of redundancy needed for the proper operation of the introduced protection scheme.

Due to the fact that each acquired waveform is manipulated in phasor form, it is evident that the introduced protection scheme monitors 48 measured quantities for this example. It should be noted that internal calculations use the rectangular representation of phasors. Apart from the 48 actual measurements, there are also 6 virtual and 12 pseudo measurements, which brings the total number of monitored measurements n_z to 66. A summary is provided in Table 7.3.

Each single-phase transformer model contains five complex state variables. Therefore, the total number of states n_x within the three protection zones monitored for this study is

Table 7.3: First Microgrid Test System: Measurements

Measurement Type	Total Number
Actual	48
Derived	0
Virtual	6
Pseudo	12
Total (n_z)	66

30, which means that the redundancy coefficient R_c equals 2.2 in this example.

7.1.3 Compromised data

Attack and recorded waveforms

The first scenario to be demonstrated relies on the hypothesis that an attacker successfully manages to change the setting of the Current Transformer (CT) monitoring $i_{\mathrm{TR1,3}}$ from 5:1 to 25:1 exactly 240 ms into the simulation.

Any relay monitoring the affected transformer $\mathrm{TR1}$ only has visibility to the six measurements recorded within the protection zone, i.e., $i_{\mathrm{TR1,1}}$, $i_{\mathrm{TR1,2}}$, $i_{\mathrm{TR1,3}}$, $i_{\mathrm{TR1,4}}$, $v_{\mathrm{TR1,1}}$ and $v_{\mathrm{TR1,2}}$. The received waveforms are shown in Figures 7.3 and 7.4 with the interval between 240 ms and 250 ms highlighted. For comparison purposes, the plots for the corresponding voltages and currents of the $\mathrm{TR2}$ transformer, which operates normally, are provided in Figures 7.5 and 7.6.

The role of any relay assigned to protecting the affected transformer is to continuously receive and analyze measurements. In this case, the waveforms in Figures 7.3 and 7.4 pose a threat to both settingless relays and more traditional protection schemes. Specifically, a settingless relay would be performing DSE in the time domain continuously, thus concluding that the measurements do not fit the system model after 240 ms. A trip signal would be issued as a result, even though the transformer is healthy. Similar behavior is expected from legacy protection schemes such as differential protection, due to the fact that the algebraic sum of all currents entering the transformer is far from zero after 240 ms. Thus, the threat

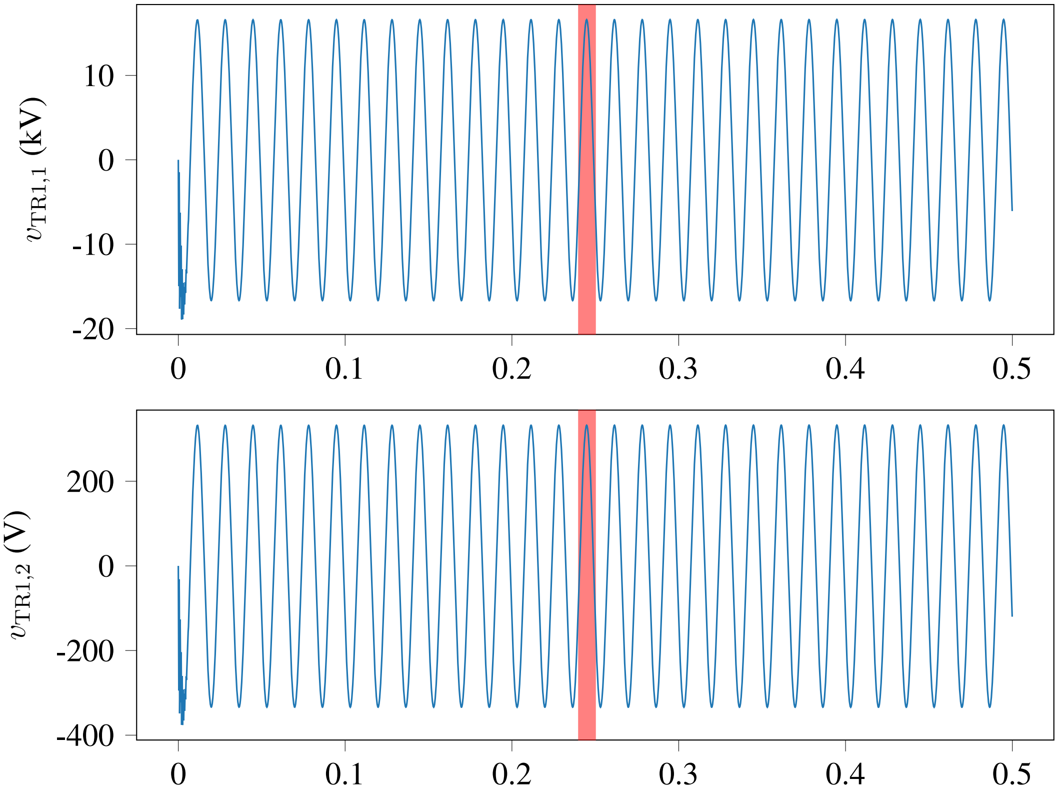

Figure 7.3: Voltage waveforms recorded at the affected transformer.

of FDIAs to both settingless and traditional relays is clear, since individual zone relays are programmed to react to these recorded waveforms by disconnecting healthy parts of the system.

The advantage of the proposed novel centralized protection scheme is that it combines measurements from multiple zones in order to protect against erroneous tripping. Hence, the addition of the proposed supervisory layer increases the security of the microgrid. Figures 7.7 and 7.8 show the calculated phasors for the same quantities as in Figures 7.3 and 7.4, which are the two voltage and four current measurements $v_{\mathrm{TR1,1}}$, $v_{\mathrm{TR1,2}}$, $i_{\mathrm{TR1,1}}$, $i_{\mathrm{TR1,2}}$, $i_{\mathrm{TR1,3}}$, $i_{\mathrm{TR1,4}}$, in conjunction with the redundant measurements $i'_{\mathrm{TR1,3}}$ and $v'_{\mathrm{TR1,2}}$. Since this figure contains both the manipulated measurement stream $i_{\mathrm{TR1,3}}$ and the redundant measurement stream $i'_{\mathrm{TR1,3}}$, the attack can be visually observed. The introduced centralized protection algorithm utilizes DSE to reach the same conclusion.

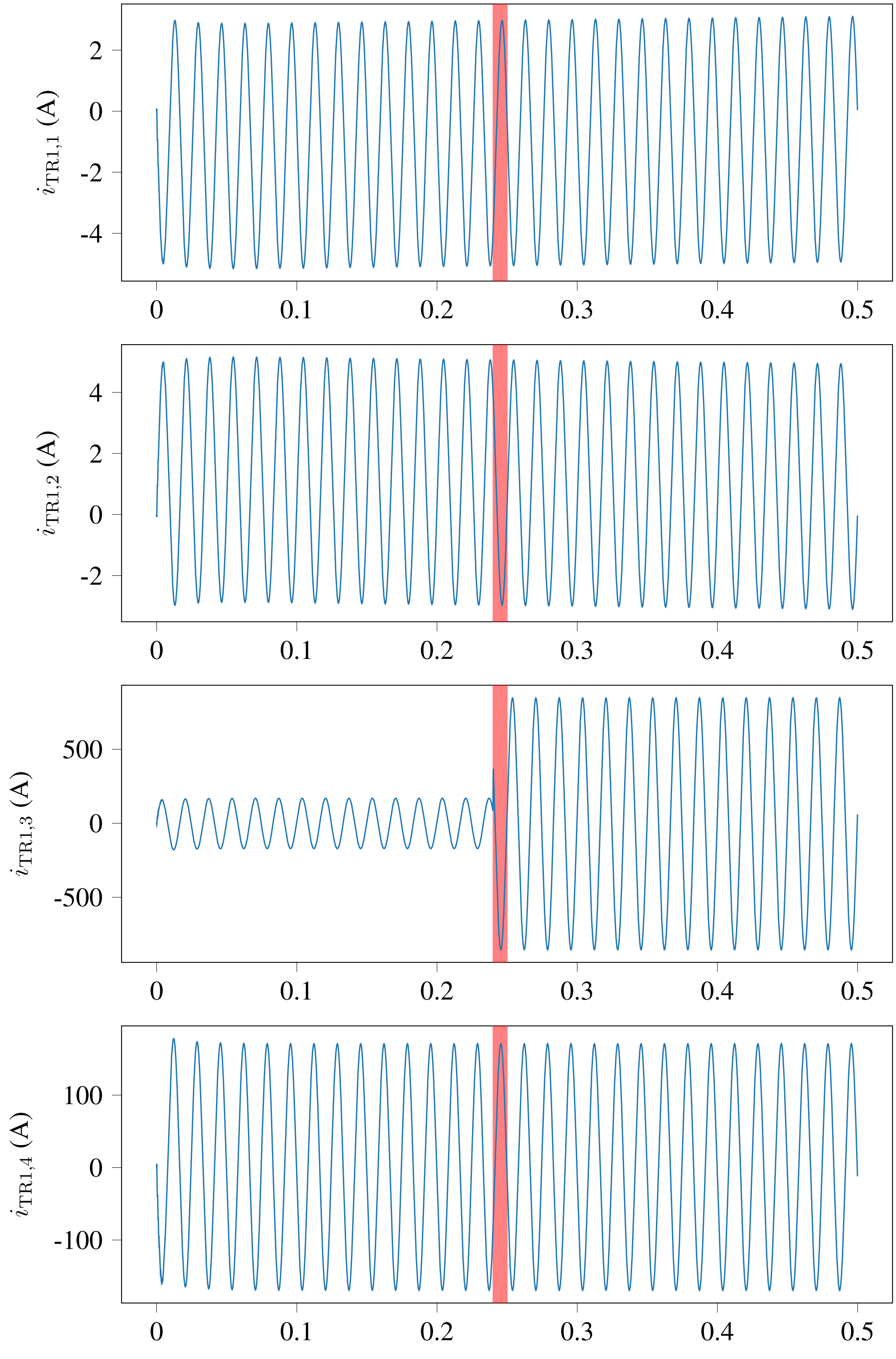

Figure 7.4: Current waveforms recorded at the affected transformer.

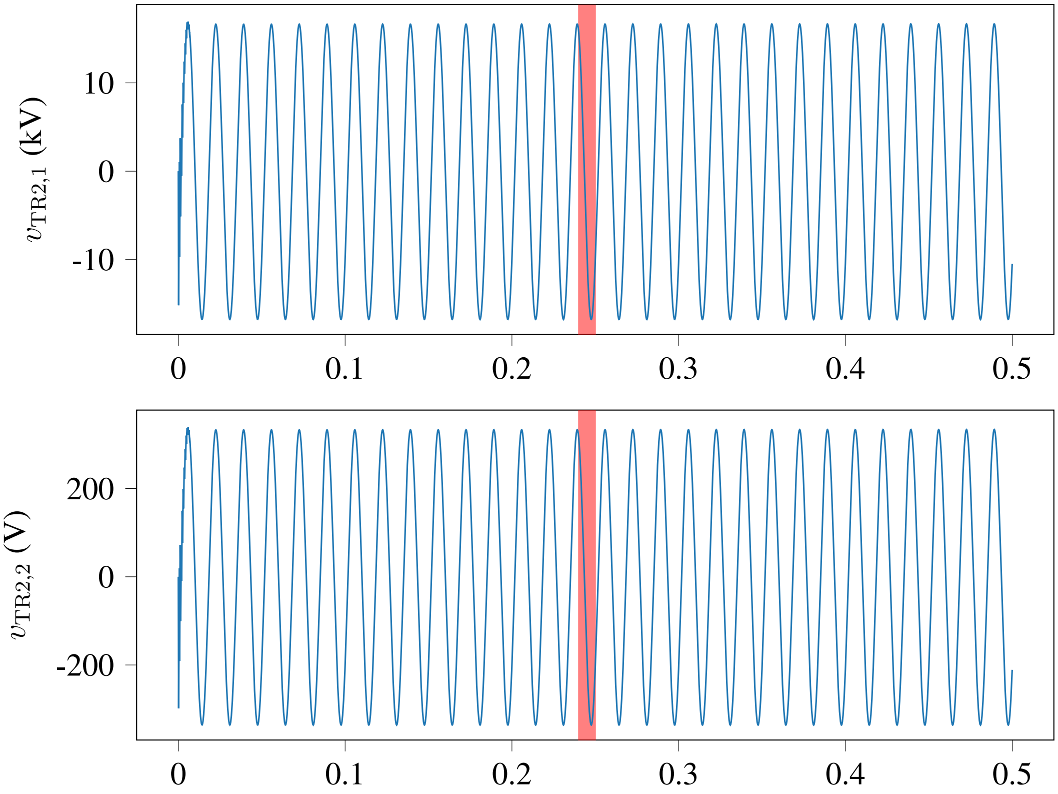

Figure 7.5: Voltage waveforms recorded at a non-affected transformer.

Protection algorithm execution

The first prerequisite of the protection process is the formation of a microgrid measurement model. The object-oriented process introduced in the previous chapters combines knowledge of individual device models, microgrid topology, and installed IEDs to fulfill this requirement in an automated way.

Once a microgrid measurement model is created, the novel protection scheme performs DSE twice per cycle, and, as expected, finds a confidence level of 100% at every instance it is run before 240 ms. The first time the DSE procedure is performed after the attack occurs is at 242 ms. First, the phasor calculation step is performed. Here, samples that span a full cycle (roughly 17 ms for this 60 Hz system) are used, so the effect of the attack on the calculated phasors is not yet clearly evident. Therefore, the confidence level remains high, as the obtained phasors still fit the system model.

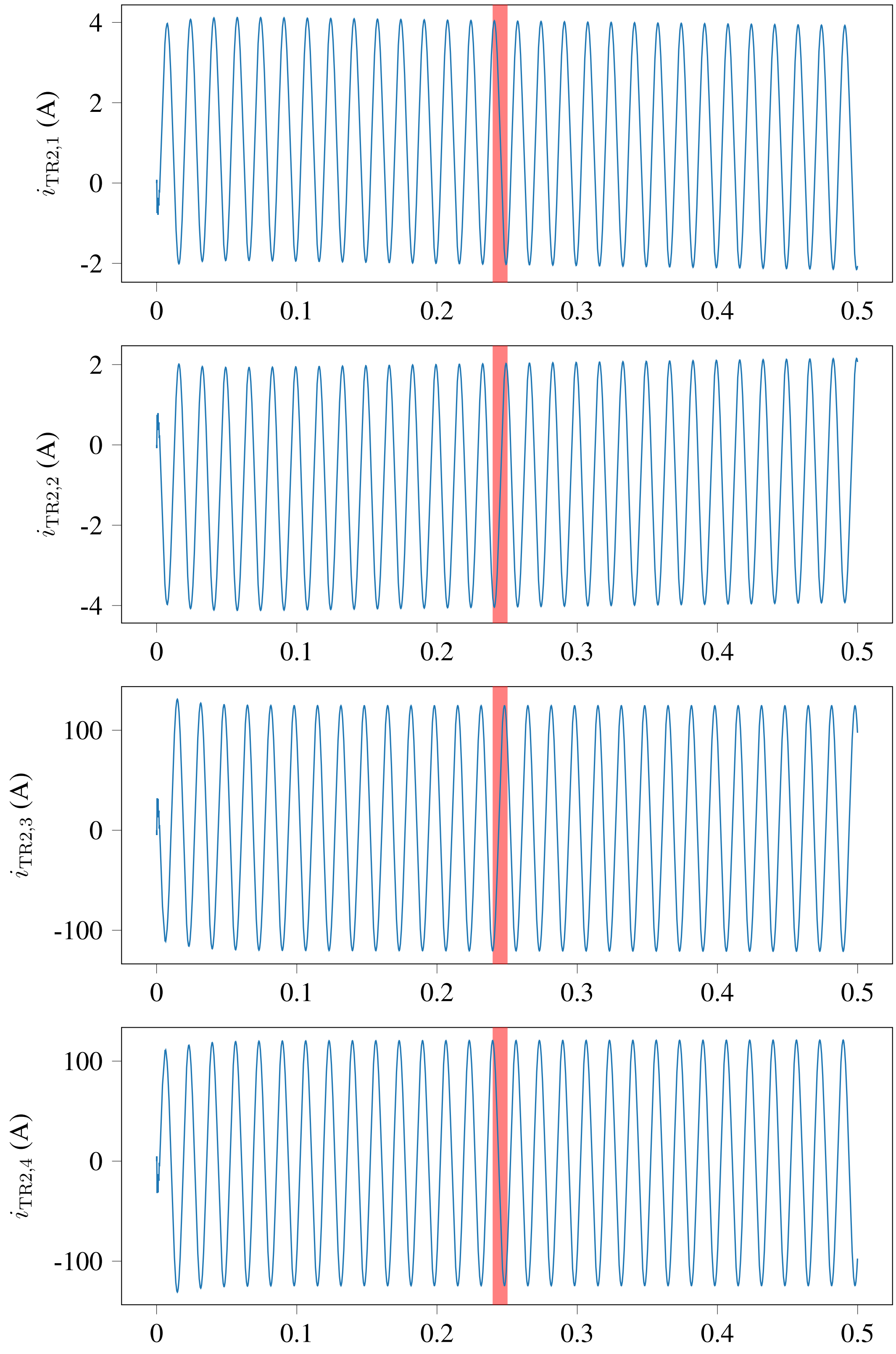

Figure 7.6: Current waveforms recorded at a non-affected transformer.

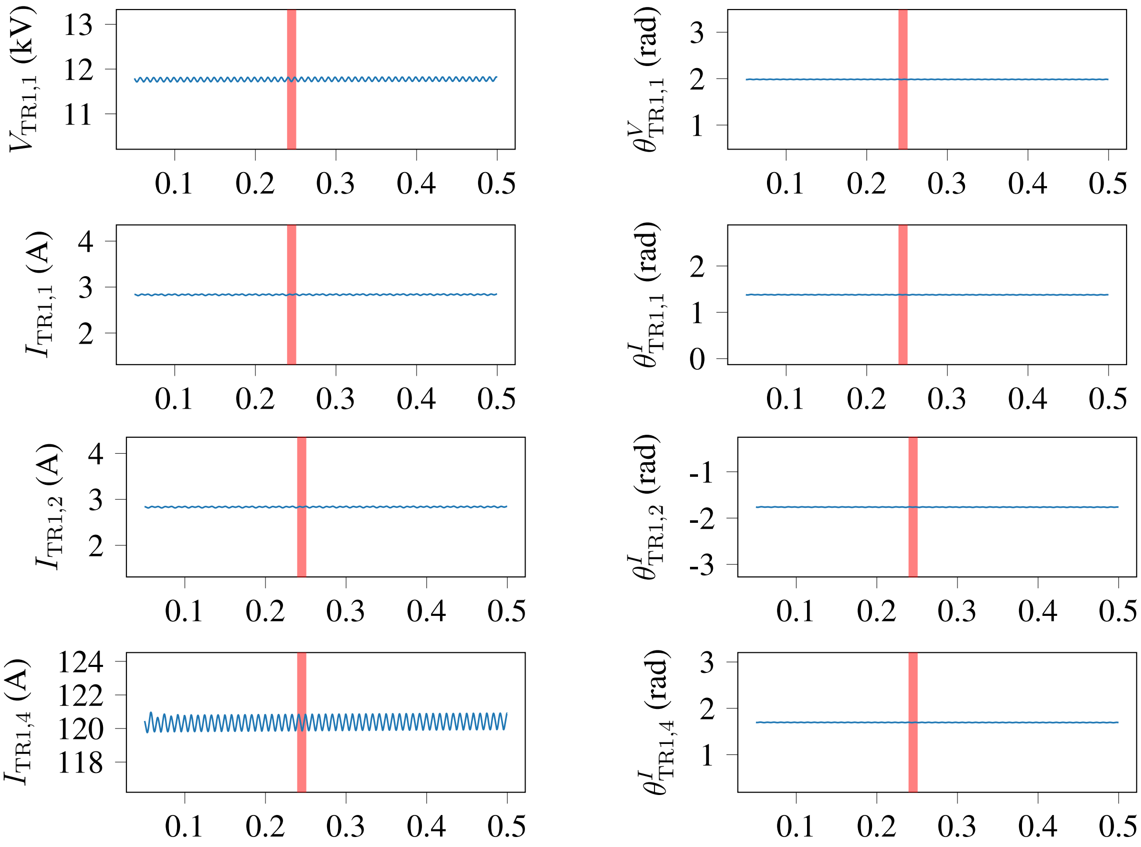

Figure 7.7: Calculated phasors for the affected transformer.

The DSE execution is repeated at 250 ms. This time, the phasor corresponding to the $i_{\text{TR1,3}}$ current measurement indeed causes the confidence level to drop. However, the protection scheme cannot determine what exactly is responsible for the confidence level drop without hypothesis testing.

Figure 7.9 shows the confidence level calculated by the centralized protection scheme, as well as polar phasor measurements and the corresponding rectangular absolute normalized residuals for the $i_{\text{TR1,3}}$ measurement channel. Here, the internal calculations of the protection scheme are performed with the hypothesis testing module deactivated for comparison purposes.

Before the start of the cyber-attack, the confidence level remains over 99.999999%, which clearly indicates that every protection zone is healthy. At the 242 ms execution step,

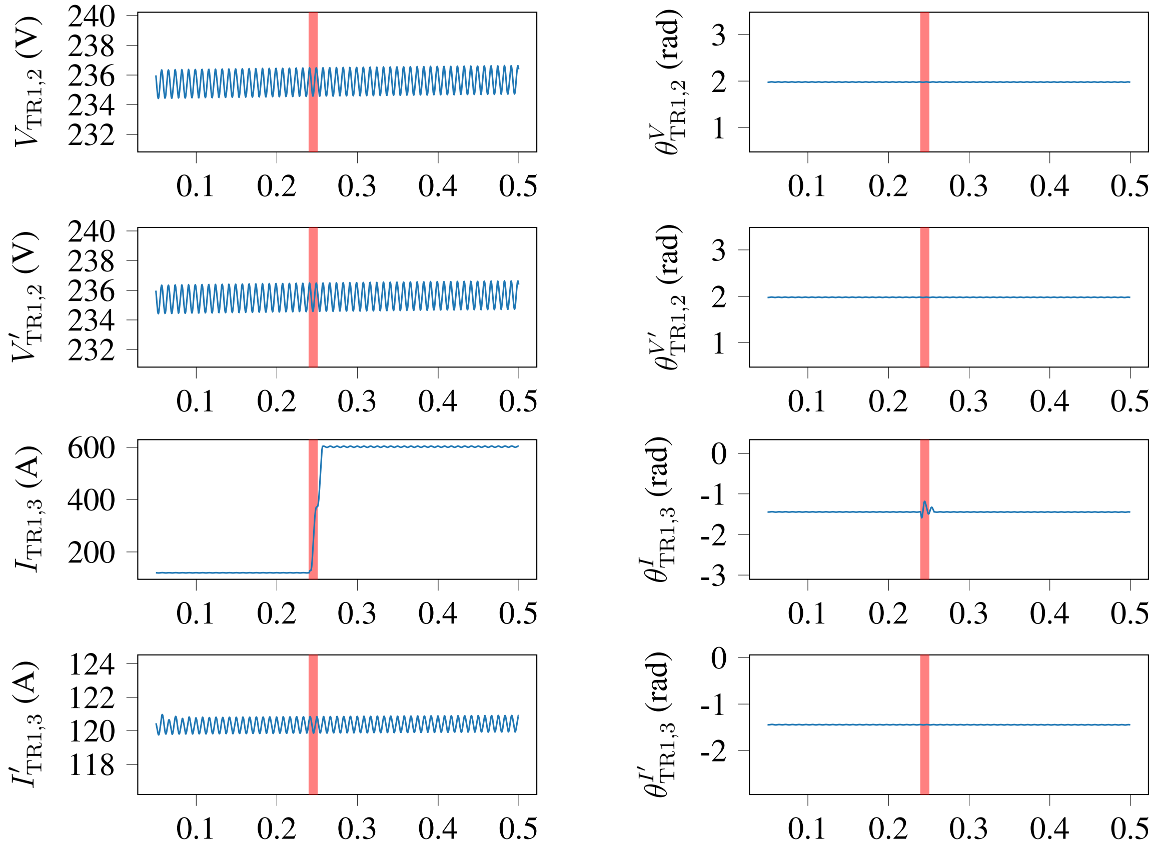

Figure 7.8: Calculated phasors for the affected transformer (with redundancy).

the confidence level drops very slightly to approximately 99.974%. At the next step, the confidence level collapses to less than 0.1%.

During DSE execution, the absolute normalized residual r_n is calculated for each measurement. Hypothesis testing relies on these values to identify suspect measurements. Figure 7.10 shows the largest absolute normalized residuals at 250 ms. The altered measurement $i_{\text{TR1,3}}$ is indeed exhibiting a normalized residual value much larger than all other measurements. The magnitude difference between the $i_{\text{TR1,3}}$ residual and the second largest residual visually confirms that the absolute normalized residual r_n is a good metric for suspect measurement identification.

In this example, each measurement is considered its own measurement channel, so $i_{\text{TR1,3}}$ is eliminated. Thus, the microgrid measurement model needs to be updated. It

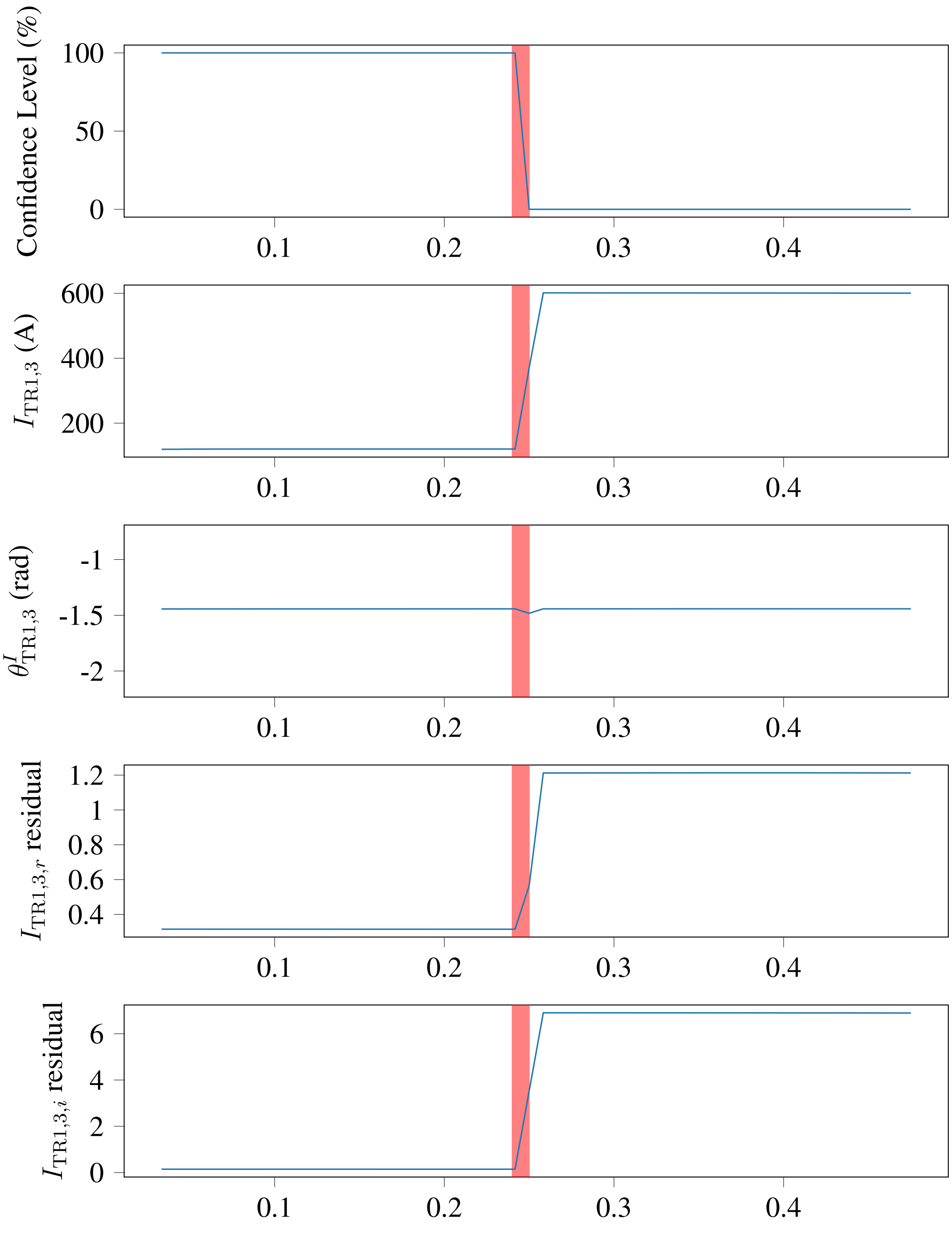

Figure 7.9: Microgrid confidence level, $i_{\mathrm{TR1,3}}$ measurements, and corresponding absolute normalized residuals (without hypothesis testing).

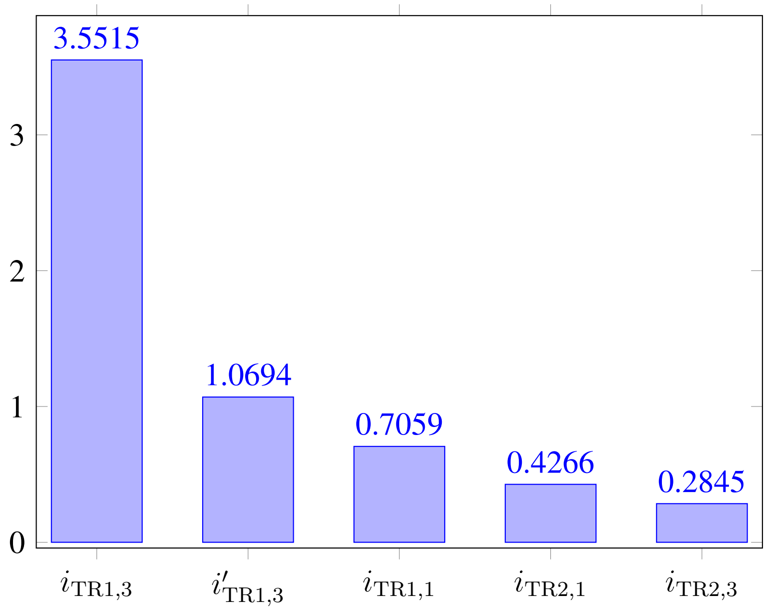

Figure 7.10: Absolute normalized residuals.

now contains every measurement it originally contained minus $i_{\mathrm{TR1,3}}$. Afterwards, DSE is run again with the rest of the calculated phasors and the reduced microgrid measurement model. The result of this step is a high confidence level, which verifies that the measurement channel $i_{\mathrm{TR1,3}}$ is compromised. Of course, during the execution of the DSE module every intermediate quantity is calculated including the absolute normalized residuals of the reduced microgrid measurement model.

Figure 7.11 shows the same quantities as Figure 7.9, but this time with the hypothesis testing and measurement elimination module activated. The reader may observe that the confidence level is indeed restored, when the hypothesis testing module gets activated, which means that the corresponding normalized residuals of the removed measurement are now equal to zero.

Two further pairs of figures are offered for comparison. Figures 7.12 and 7.13 show $i'_{\mathrm{TR1,3}}$, which is the redundant measurement of the attacked measurement $i_{\mathrm{TR1,3}}$, as well as the corresponding protection calculations both without and with the hypothesis testing module. These two figures demonstrate that when the attack happens, all internal calculations for the first transformer protection zone exhibit signs of the attack. However, the

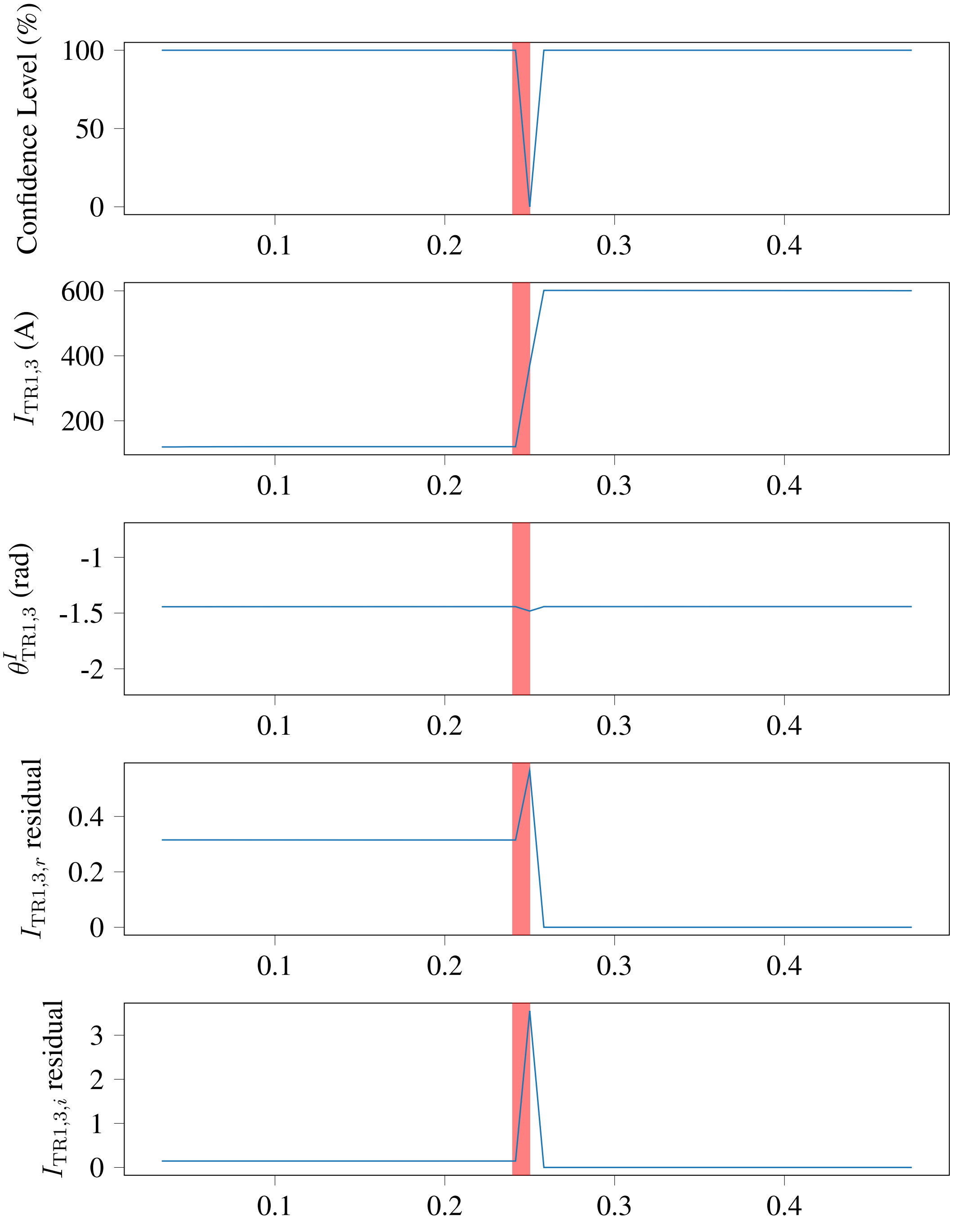

Figure 7.11: Microgrid confidence level, $i_{\mathrm{TR1,3}}$ measurements, and corresponding absolute normalized residuals (with hypothesis testing).

measurement elimination step allows the absolute normalized residuals of the $i'_{\mathrm{TR1,3}}$ measurement to return to their pre-attack values, thus verifying that the protection zone remains healthy.

Moreover, Figures 7.14 and 7.15 show that the attack in one protection zone has no effect on the behavior and the internal calculations of the $\mathrm{TR2}$ transformer protection zone. There, both the recorded measurements and the calculated absolute normalized residuals remain steady throughout the time interval.

Once the FDIA is detected, the introduced protection scheme reacts by notifying the system operator while also blocking the relay monitoring the affected transformer $\mathrm{TR1}$ from tripping. This goal is achieved within just 10 ms after the initialization of measurement tampering, which ensures that the centralized protection scheme can react quickly enough to prevent the intervention of the individual zone relay and maintain normal system operation.

7.1.4 Transformer fault

Power fault and recorded waveforms

The second scenario to be simulated shows the behavior of the novel scheme in the presence of a fault within one of the monitored individual protection zones. Here, a segment of the secondary winding of the $\mathrm{TR1}$ transformer containing 5% of its total turns is assumed to be short-circuited at 240 ms.

As was the case with the cyber-attack case, the protection relay monitoring the faulty transformer $\mathrm{TR1}$ will have access to the same six zone measurements, namely $i_{\mathrm{TR1,1}}$, $i_{\mathrm{TR1,2}}$, $i_{\mathrm{TR1,3}}$, $i_{\mathrm{TR1,4}}$, $v_{\mathrm{TR1,1}}$ and $v_{\mathrm{TR1,2}}$. These waveforms are presented in Figures 7.16 and 7.17 with the interval between 240ms and 250ms highlighted. Again, the plots for the corresponding voltages and currents of the $\mathrm{TR2}$ transformer, which operates normally, are provided in Figures 7.18 and 7.19 for comparison purposes.

Once more, all three protection zones, including the $\mathrm{TR1}$ transformer zone, are moni-

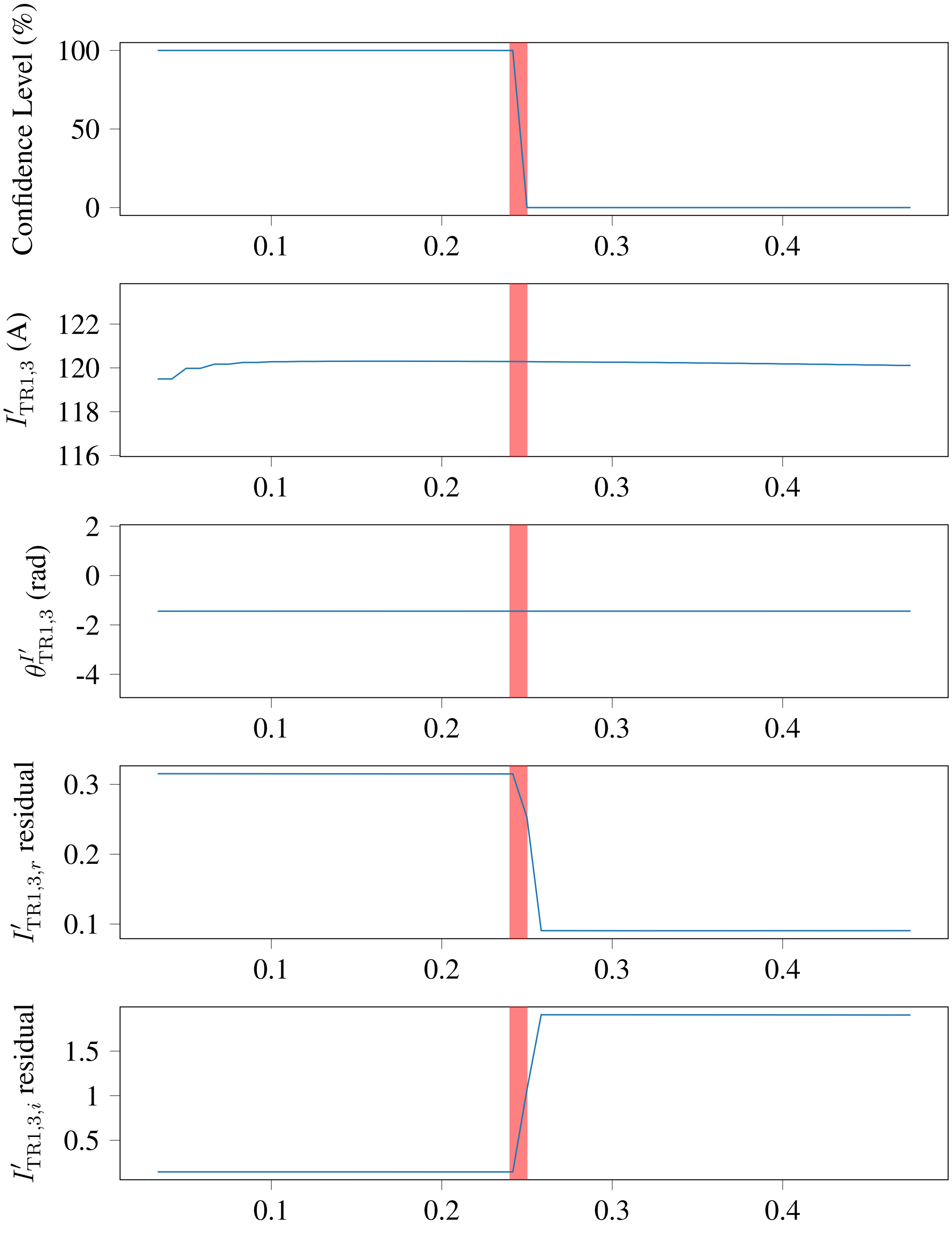

Figure 7.12: Microgrid confidence level, $i'_{\mathrm{TR1,3}}$ measurements, and corresponding absolute normalized residuals (without hypothesis testing).

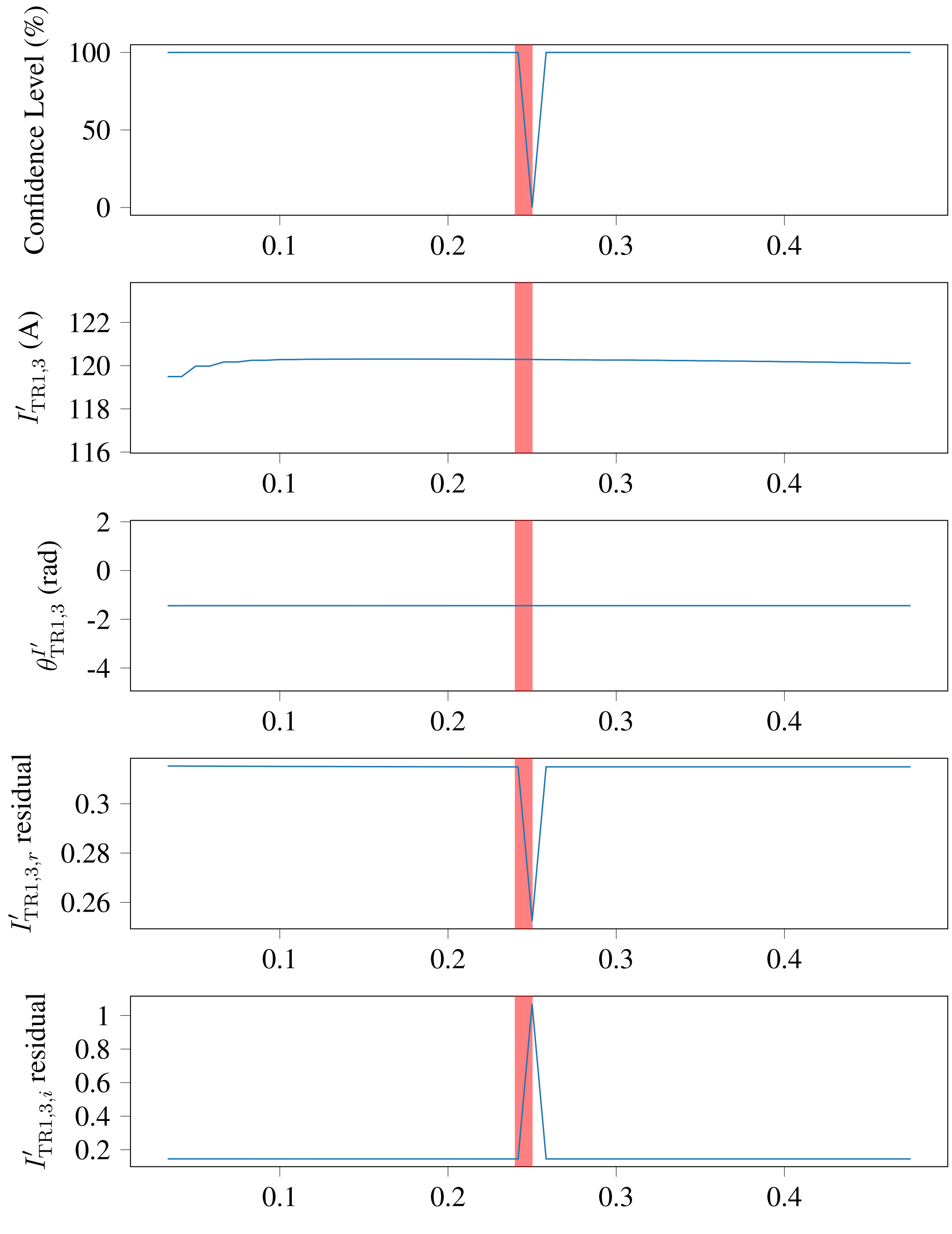

Figure 7.13: Microgrid confidence level, $i'_{\mathrm{TR1,3}}$ measurements, and corresponding absolute normalized residuals (with hypothesis testing).

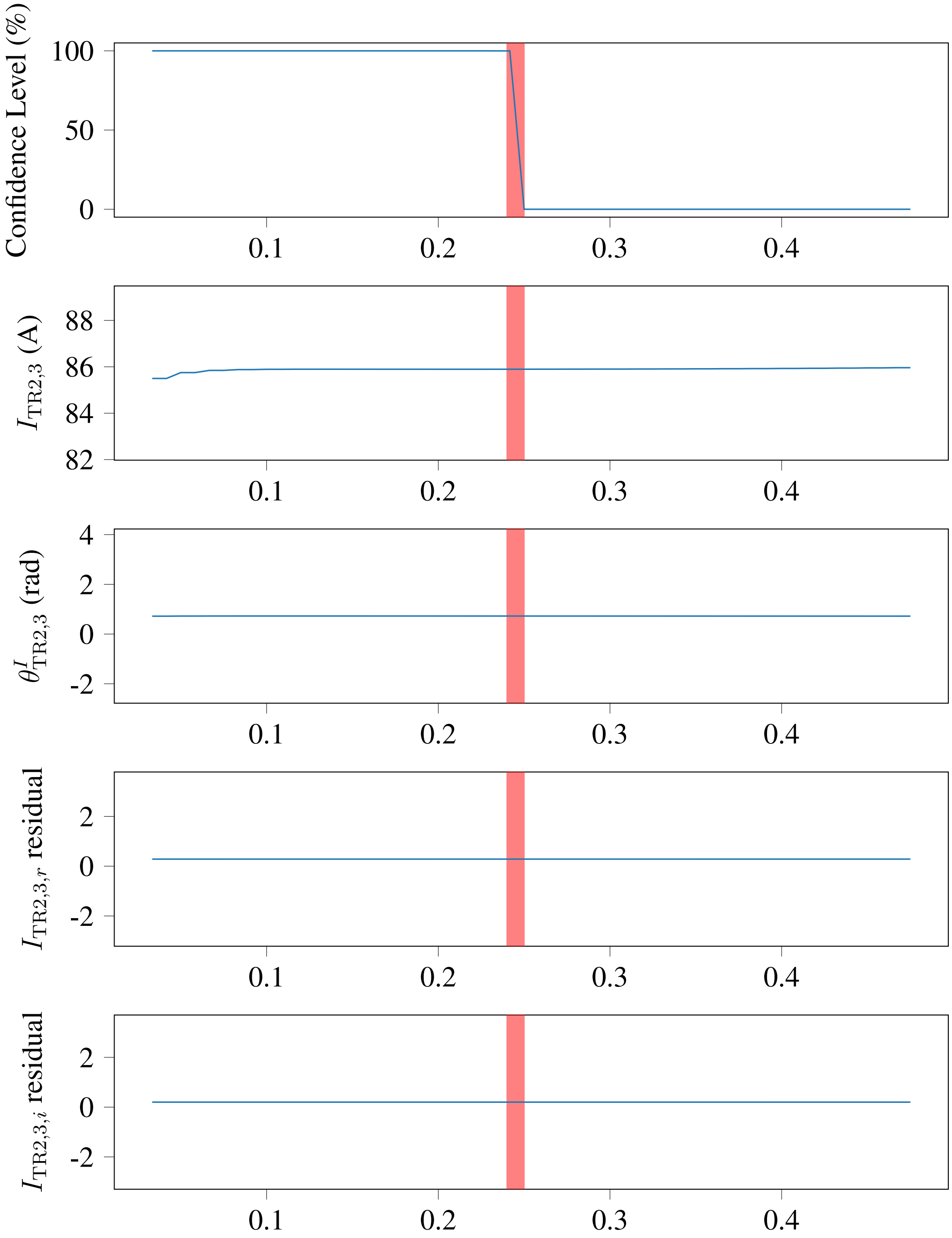

Figure 7.14: Microgrid confidence level, $i_{\mathrm{TR}2,3}$ measurements, and corresponding absolute normalized residuals (without hypothesis testing).

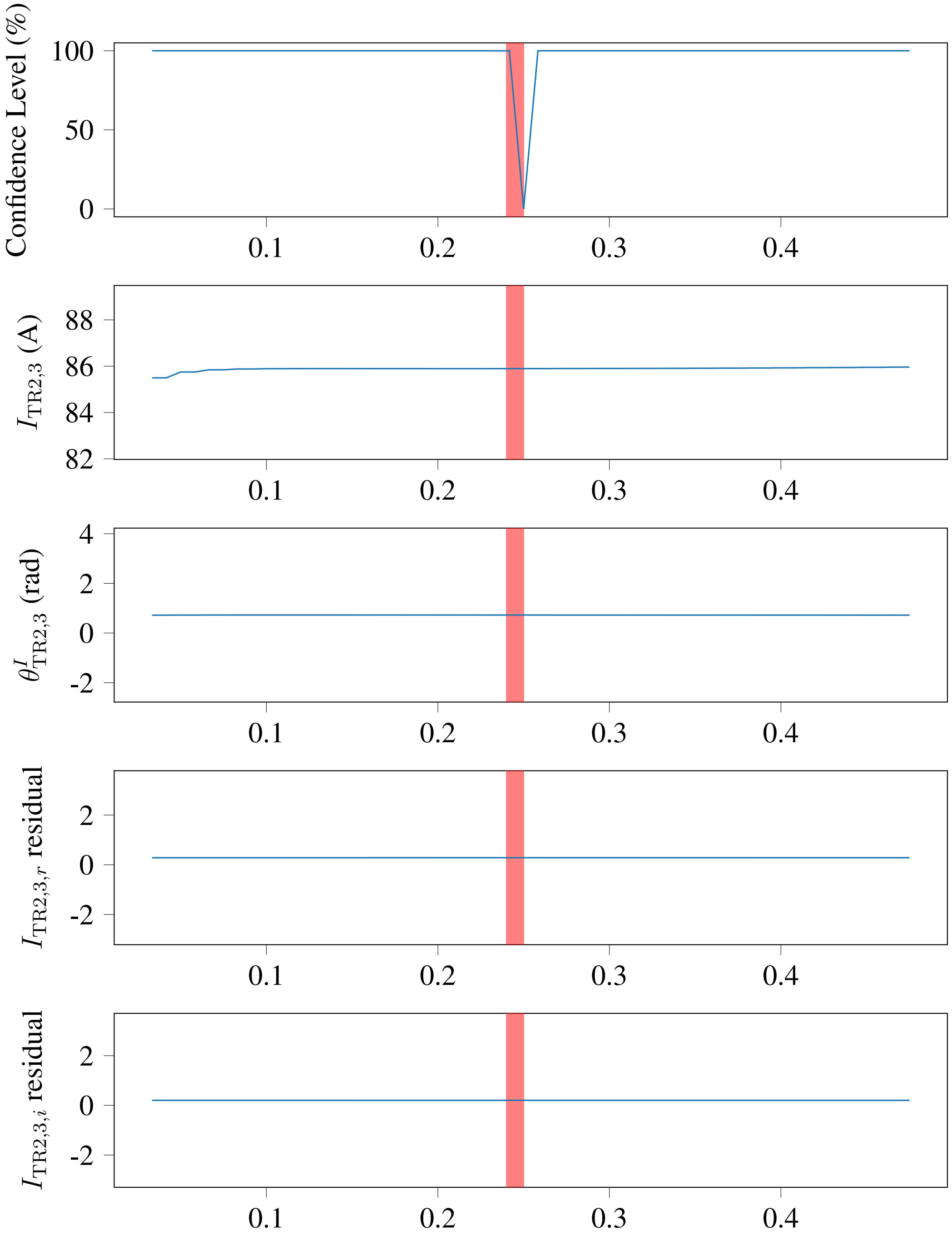

Figure 7.15: Microgrid confidence level, $i_{\mathrm{TR2,3}}$ measurements, and corresponding absolute normalized residuals (with hypothesis testing).

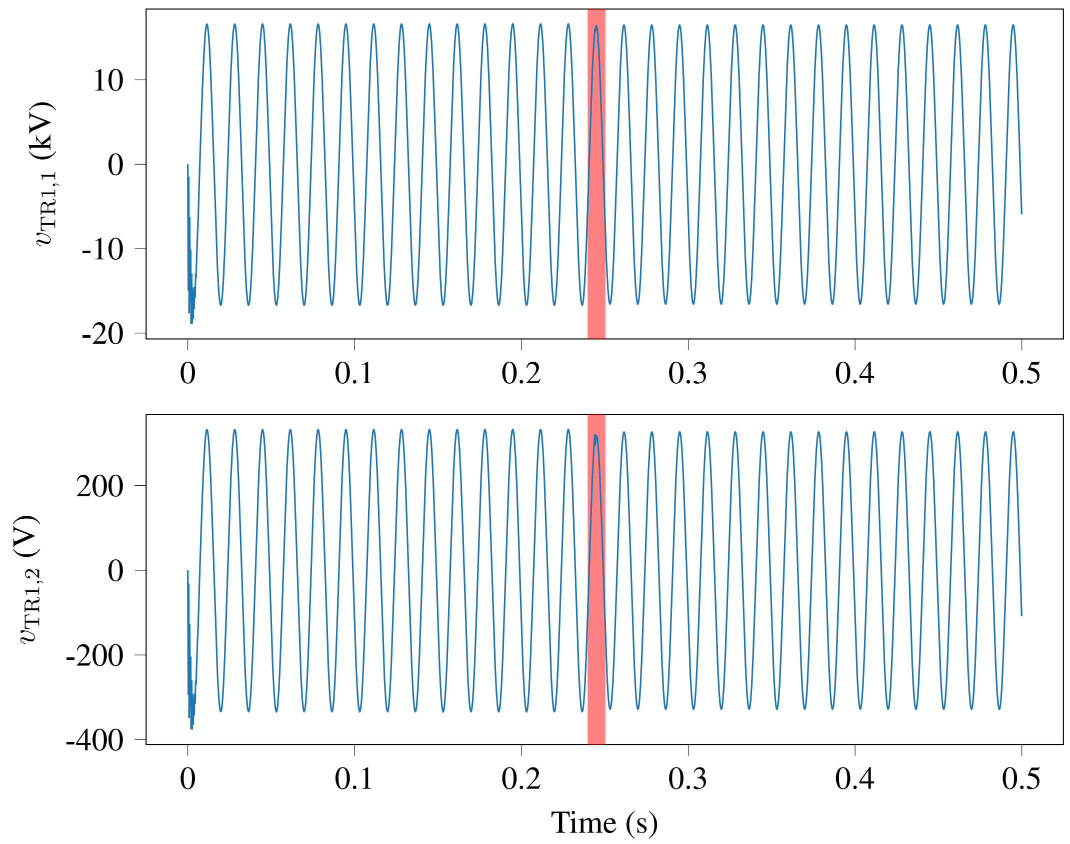

Figure 7.16: Voltage waveforms recorded at the faulty transformer.

tored by relays that continuously analyze measurement samples based on prespecified protection logic. Since the recorded measurements do not fit the model of a healthy transformer after 240 ms, a settingless relay monitoring the affected protection zone is once again expected to send a trip signal to the zone breakers. The same conclusion may also be reached by relays that implement legacy protection schemes, although it should be noted that this type of fault is specifically chosen because it is hard to be detected by legacy schemes. Since a legitimate power fault exists within a monitored protection zone in this scenario, the proposed centralized protection scheme should not interfere with the tripping action of any individual zone relay that detects the short-circuit. The rest of this study demonstrates that this is indeed the case.

In order to perform its supervisory functions, the proposed scheme operates in the following way. First, Figures 7.20 and 7.21 show the calculated phasors for the same quanti-

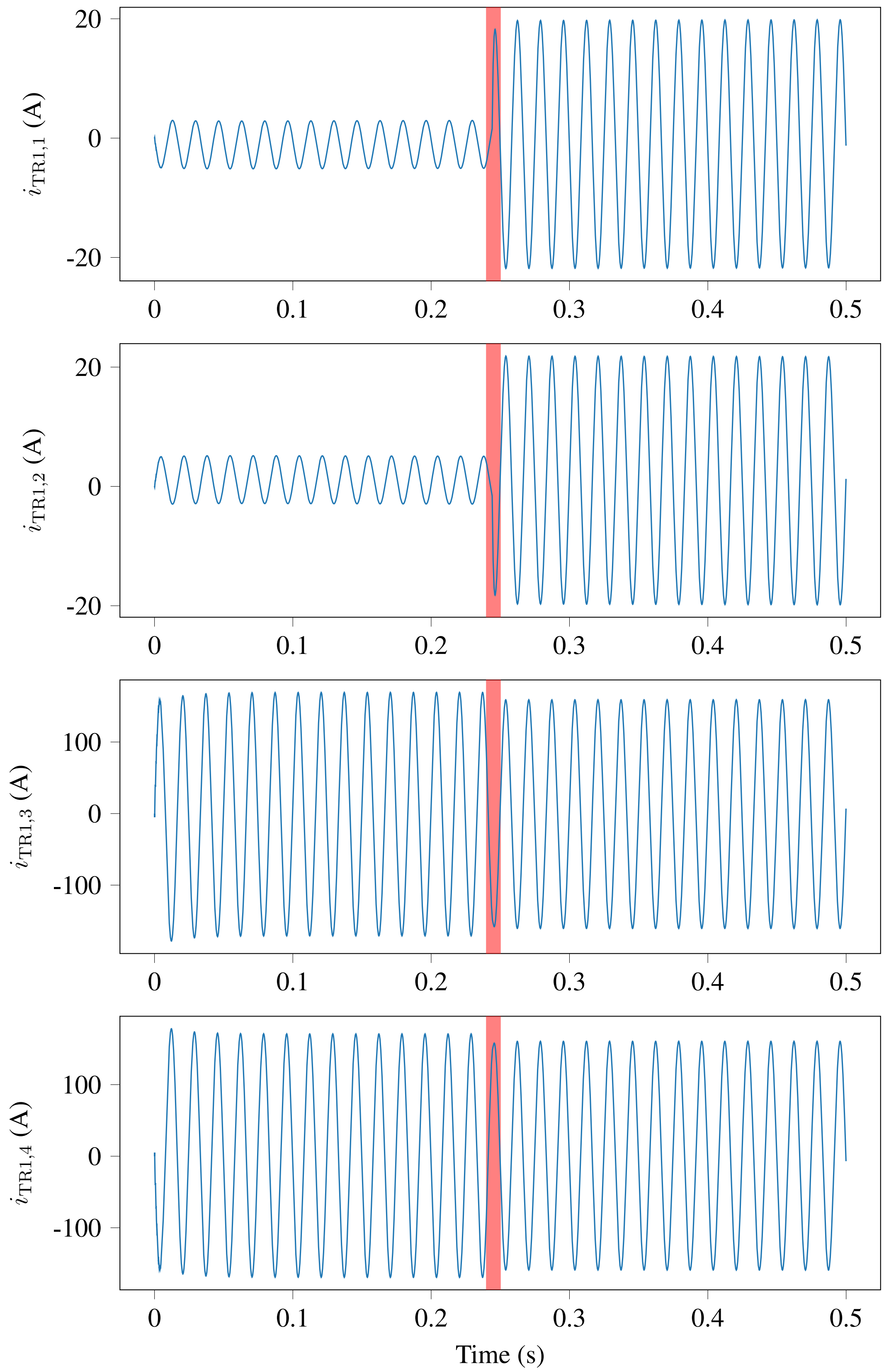

Figure 7.17: Current waveforms recorded at the faulty transformer.

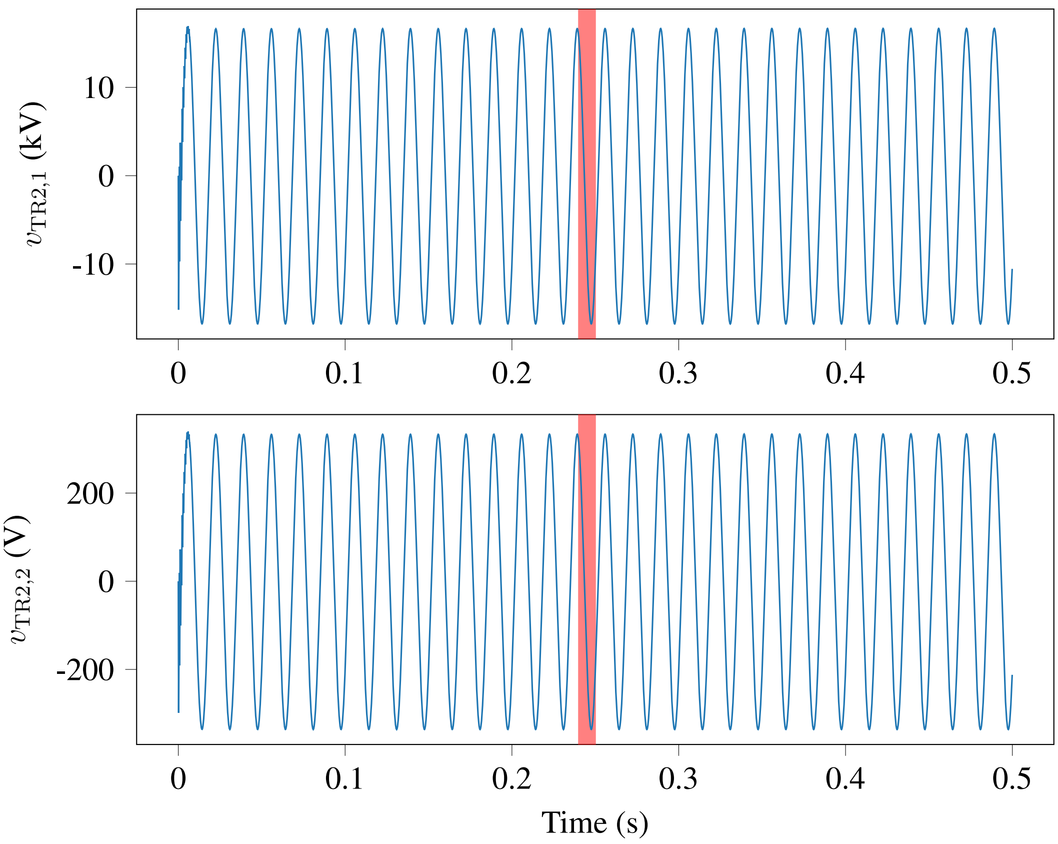

Figure 7.18: Voltage waveforms recorded at a non-faulty transformer.

ties as in Figures 7.16 and 7.17, which are the two voltage and four current measurements $v_{\mathrm{TR1,1}}$, $v_{\mathrm{TR1,2}}$, $i_{\mathrm{TR1,1}}$, $i_{\mathrm{TR1,2}}$, $i_{\mathrm{TR1,3}}$, $i_{\mathrm{TR1,4}}$, in conjunction with the redundant measurements $i'_{\mathrm{TR1,3}}$ and $v'_{\mathrm{TR1,2}}$. It is worth noting that the waveforms for both $i_{\mathrm{TR1,3}}$ and $i'_{\mathrm{TR1,3}}$ are essentially identical, as now both measurement channels accurately record the situation within the protection zone. The novel protection scheme utilizes DSE to detect the fault.

Protection algorithm execution

Again, the creation of a microgrid measurement model is the first step in the execution of the protection algorithm. This goal is satisfied through the already presented methodology. Moreover, the confidence level calculation at every time step before the fault initiation does indeed verify the healthy condition of all three single-phase transformers.

As was the case with the cyber-attack scenario, the execution of DSE at 242 ms still

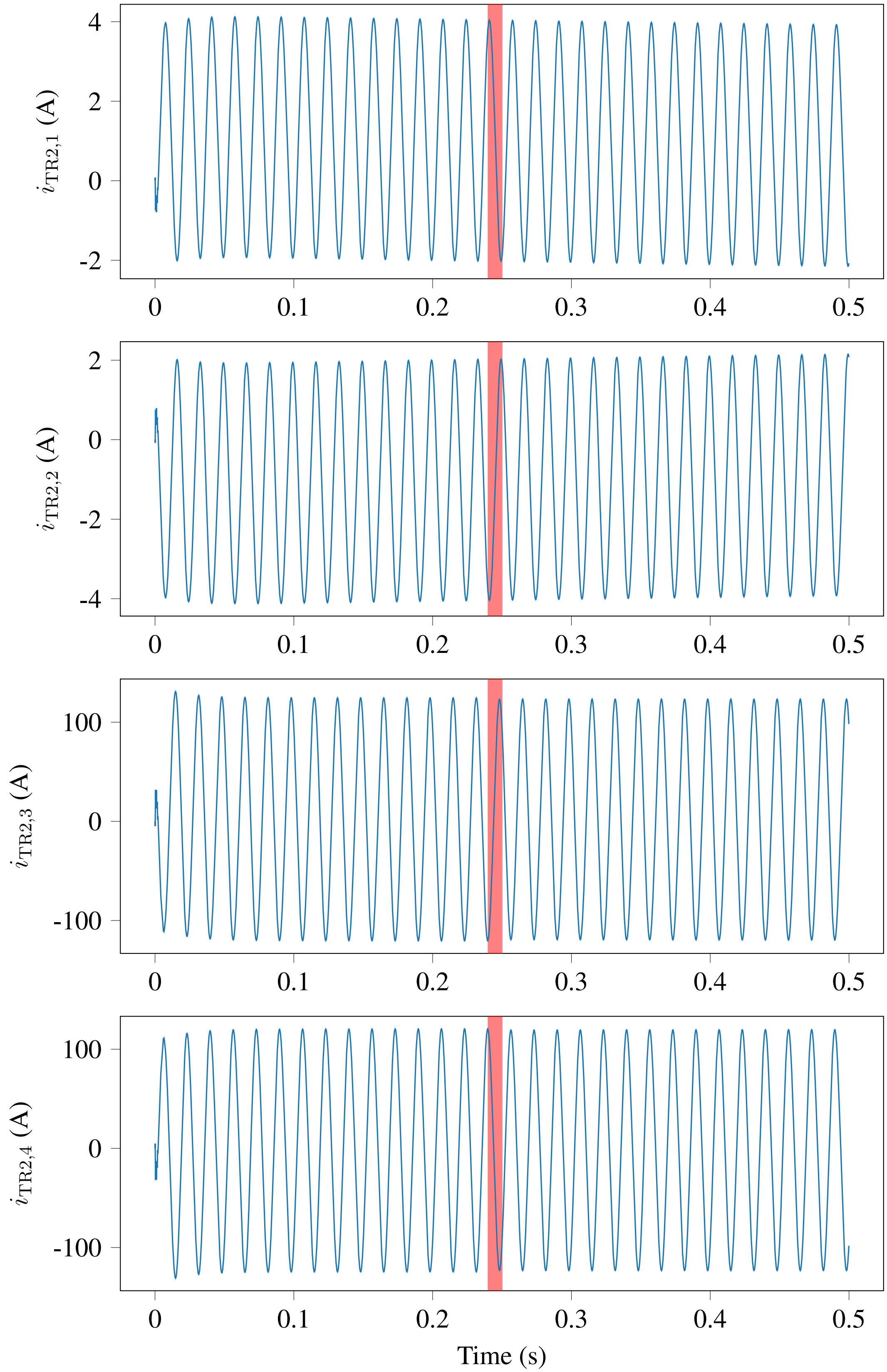

Figure 7.19: Current waveforms recorded at a non-faulty transformer.

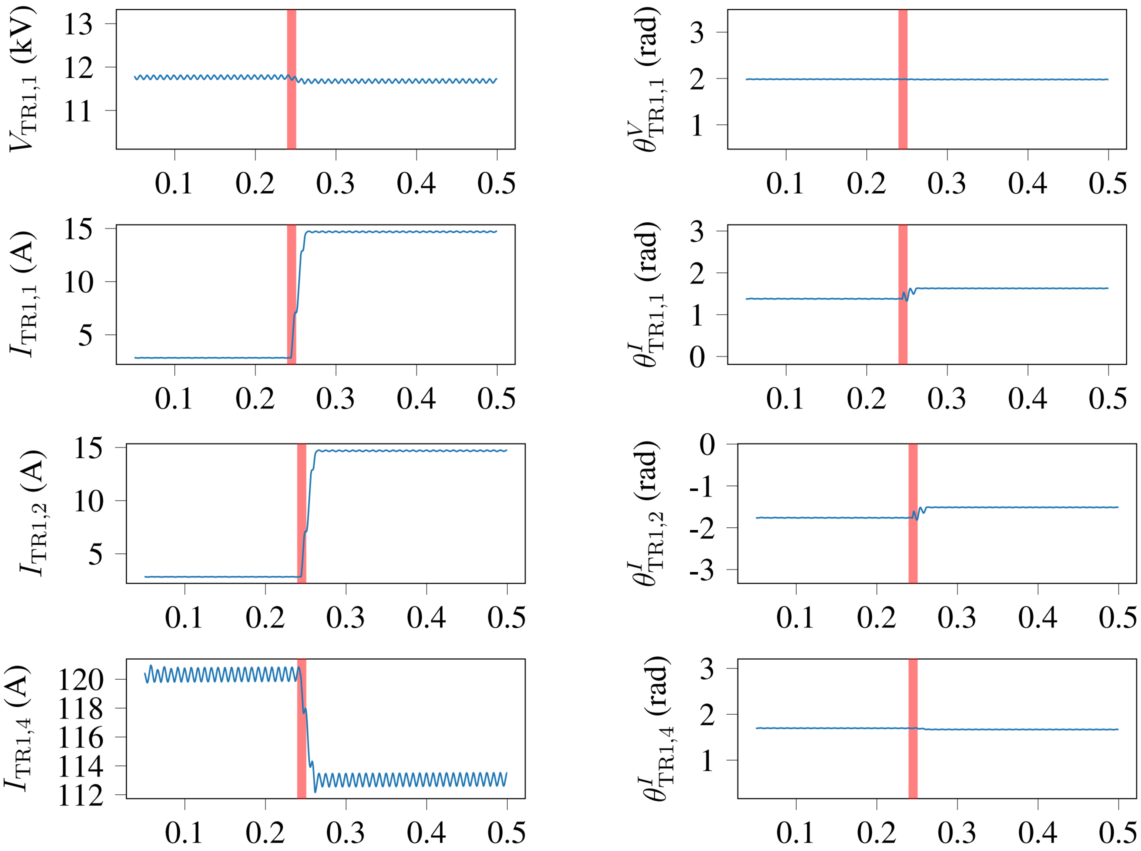

Figure 7.20: Calculated phasors for the faulty transformer.

finds a high confidence level, thus failing to trigger the centralized protection scheme. The reason for this is, again, that the phasor calculation step will not have used enough samples acquired after the fault initiation, thus resulting in phasors that fit the system model relatively well. The discrepancy between the calculated phasors and the system model will be evident at 250 ms. At this time, the confidence level will drop, therefore triggering the hypothesis testing process.

Figure 7.22 shows the confidence level calculated by the centralized protection scheme, as well as polar phasor measurements and the corresponding rectangular absolute normalized residuals for the $i_{\text{TR1,3}}$ measurement channel. Once more, the results shown here are obtained with the hypothesis testing module deactivated for comparison purposes.

As was the case with the tampered measurements scenario, before the initiation of the

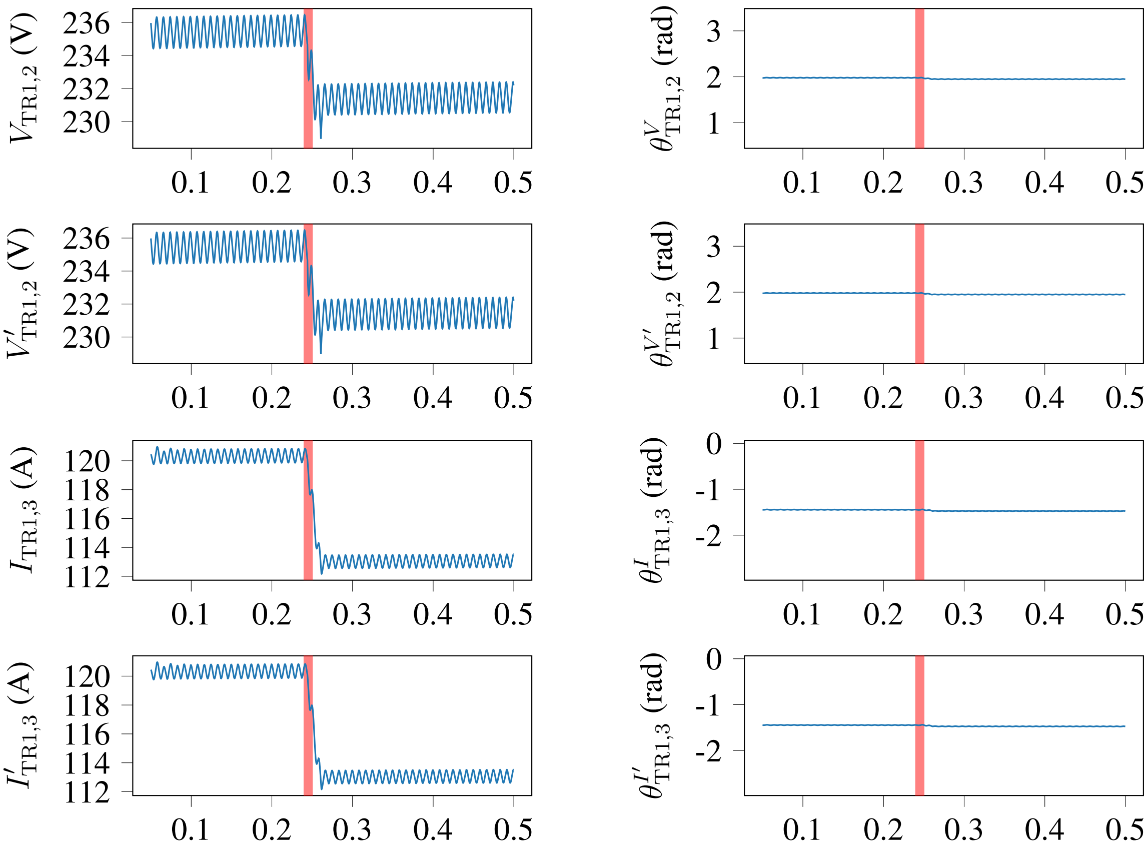

Figure 7.21: Calculated phasors for the faulty transformer (with redundancy).

power fault, the confidence level remains over 99.999999%, which clearly indicates that every protection zone is healthy. At the 242 ms execution step, the confidence level drops very to approximately 66.593%, which is a much more significant confidence level drop than the one in the tampered measurements scenario. Once again, at the next step, the confidence level collapses to less than 0.1%.

The hypothesis testing module starts by ordering again the absolute normalized residuals r_n for all measurements in descending order. These residuals have already been calculated during the DSE execution, so the computational overhead is minimal. The largest absolute normalized residuals r_n here correspond to measurements recorded at the transformer $\mathrm{TR1}$. The three largest ones are presented in Figure 7.23 alongside similar residuals from the other protection zones for comparison purposes. It is worth noting that there is a

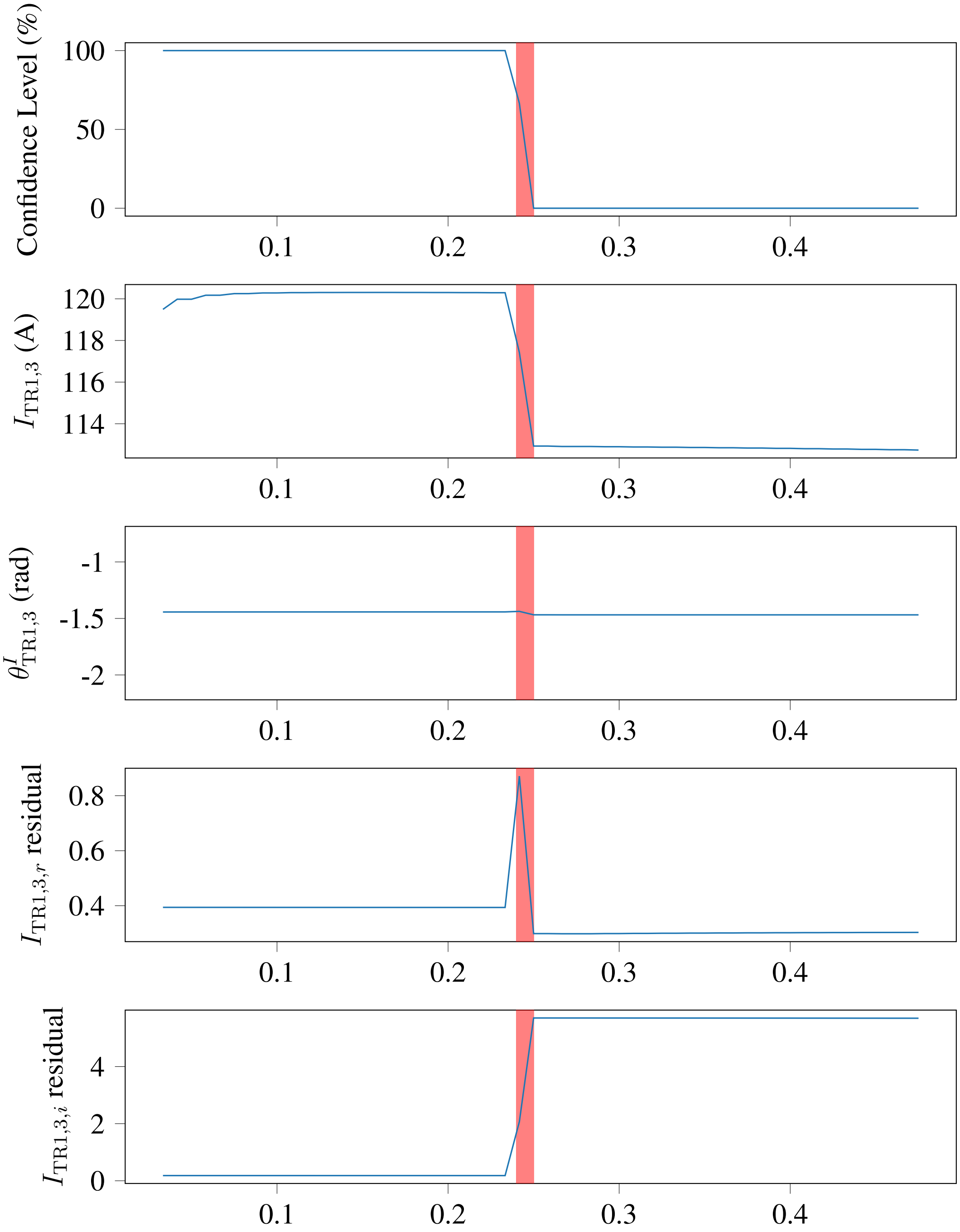

Figure 7.22: Microgrid confidence level, $i_{\mathrm{TR1,3}}$ measurements, and corresponding absolute normalized residuals (without hypothesis testing).

very visible magnitude gap between the two groups of residuals, which assists the operation of the novel centralized protection scheme.

Coincidentally, $i_{\mathrm{TR1,3}}$ is again the measurement with the highest normalized residual. Therefore, it is eliminated, and a new reduced microgrid measurement model is formed with all the initial measurements minus $i_{\mathrm{TR1,3}}$. Then, DSE is once again executed using the reduced microgrid measurement model. However, the elimination of this measurement is not sufficient to restore the confidence level to an acceptable value this time.

This restoration of the confidence level to 100% is achieved instead by eliminating all measurements corresponding to the affected protection zone.

Specifically, the measurements to be removed are $v_{\mathrm{TR1,1}}$, $v_{\mathrm{TR1,2}}$, $i_{\mathrm{TR1,1}}$, $i_{\mathrm{TR1,2}}$, $i_{\mathrm{TR1,3}}$, $i_{\mathrm{TR1,4}}$, $i'_{\mathrm{TR1,3}}$, and $v'_{\mathrm{TR1,2}}$, i.e., all measurements associated with the affected transformer. Furthermore, the quasi-dynamic domain transformer model used here contains one complex virtual equation, or, equivalently, two real virtual equations. These are also eliminated. The microgrid state vector x is also affected, as the $\mathrm{TR1}$ model contains one complex internal variable. Therefore, two real state variables need to be removed. Then, DSE is performed again using the updated microgrid measurement model, and a new confidence level is calculated, which is within acceptable limits. This indicates that there is indeed a discrepancy between the model of a protection zone and all corresponding measurements.

Figure 7.24 shows the same quantities as Figure 7.22, but this time with the hypothesis testing and measurement elimination module activated. It is evident that the confidence level is indeed restored upon activation of the hypothesis testing module. This also means that the corresponding normalized residuals of all removed measurements are now equal to zero.

Two further pairs of figures are offered for comparison. Figures 7.25 and 7.26 show the $i_{\mathrm{TR1,1}}$, which is another measurement of the faulty transformer, as well as the corresponding protection calculations both without and with the hypothesis testing module. Since the proposed centralized protection scheme eliminates the $i_{\mathrm{TR1,1}}$ measurement, as it belongs to

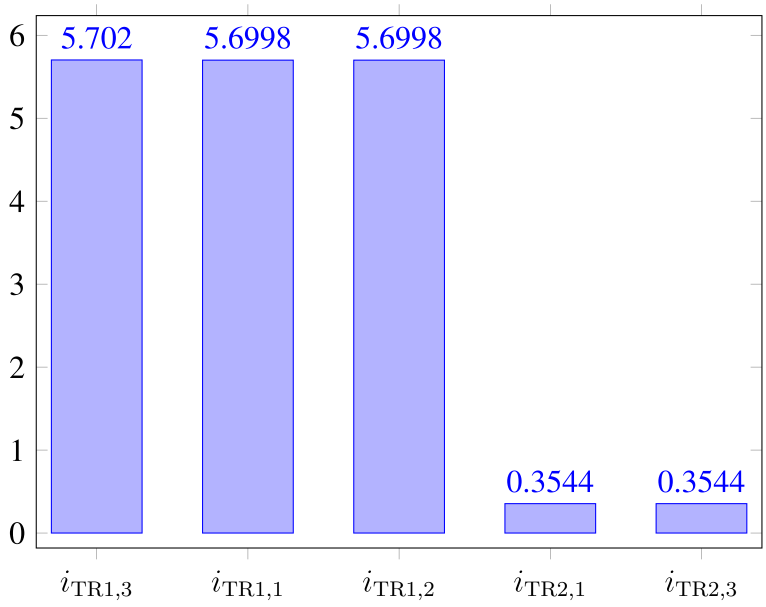

Figure 7.23: Absolute normalized residuals.

the affected transformer, the corresponding normalized residuals become equal to zero.

Just as the attack on one protection zone should not affect the operation of the proposed scheme regarding other protection zones, the same applies to power faults. Specifically, Figures 7.27 and 7.28 show that the $\mathrm{TR2}$ protection zone remains healthy, so the operation of the hypothesis testing module does not affect it.

The detected discrepancy verifies that there is a fault within this protection zone. Hence, any relay monitoring the faulty zone is allowed to trip the zone breakers for the affected transformer $\mathrm{TR1}$. Once more the reaction time of the centralized protection scheme is short enough to produce a verdict within the reaction time of the individual relay(s) responsible for clearing the fault, and proper system operation is thus maintained.

7.2 Detailed Microgrid Model

In this section a more complex microgrid that also includes detailed time domain models for DERs is examined under various scenarios.

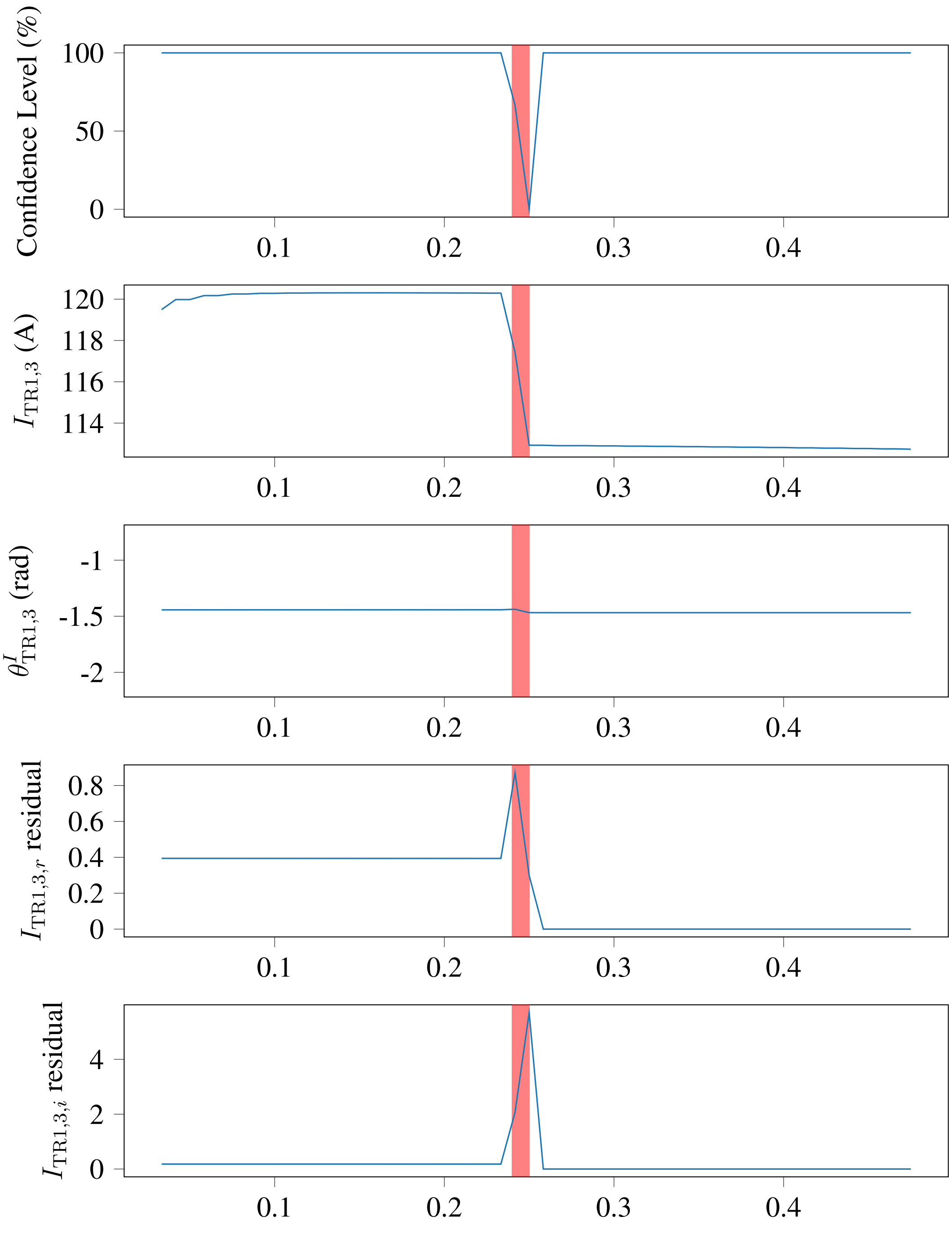

Figure 7.24: Microgrid confidence level, $i_{\mathrm{TR1,3}}$ measurements, and corresponding absolute normalized residuals (with hypothesis testing).

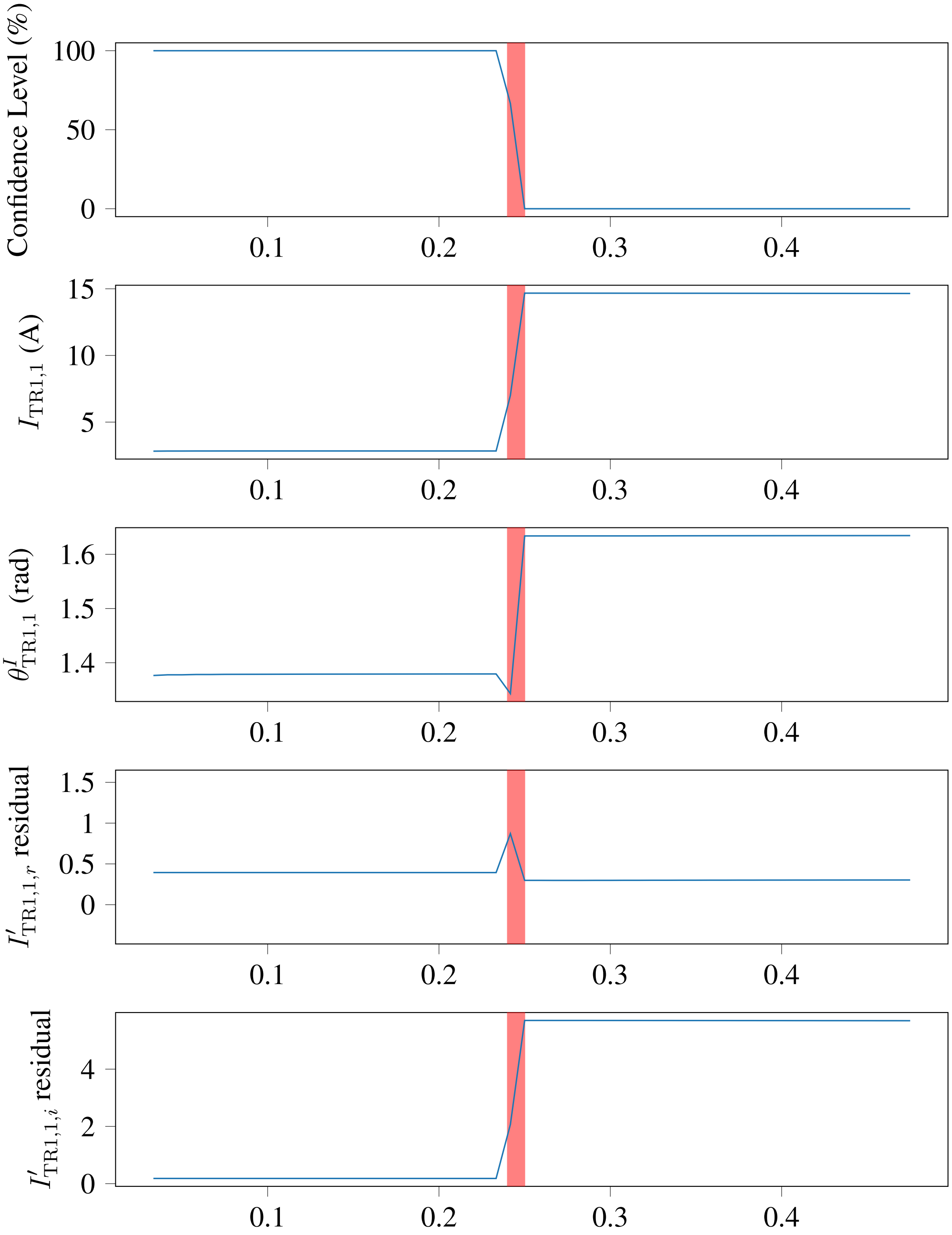

Figure 7.25: Microgrid confidence level, $i_{\mathrm{TR1,1}}$ measurements, and corresponding absolute normalized residuals (without hypothesis testing).

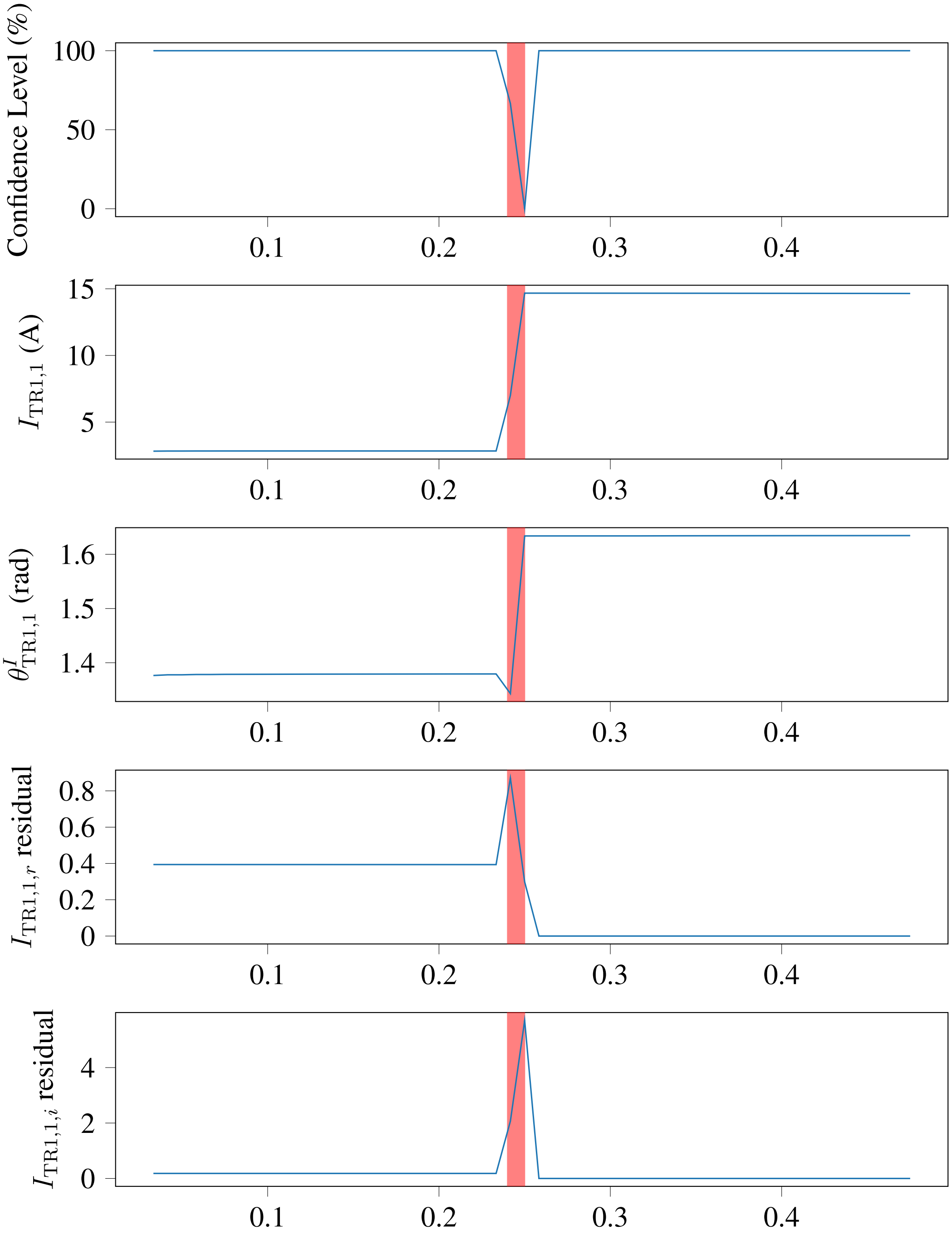

Figure 7.26: Microgrid confidence level, $i_{\text{TR}1,1}$ measurements, and corresponding absolute normalized residuals (with hypothesis testing).

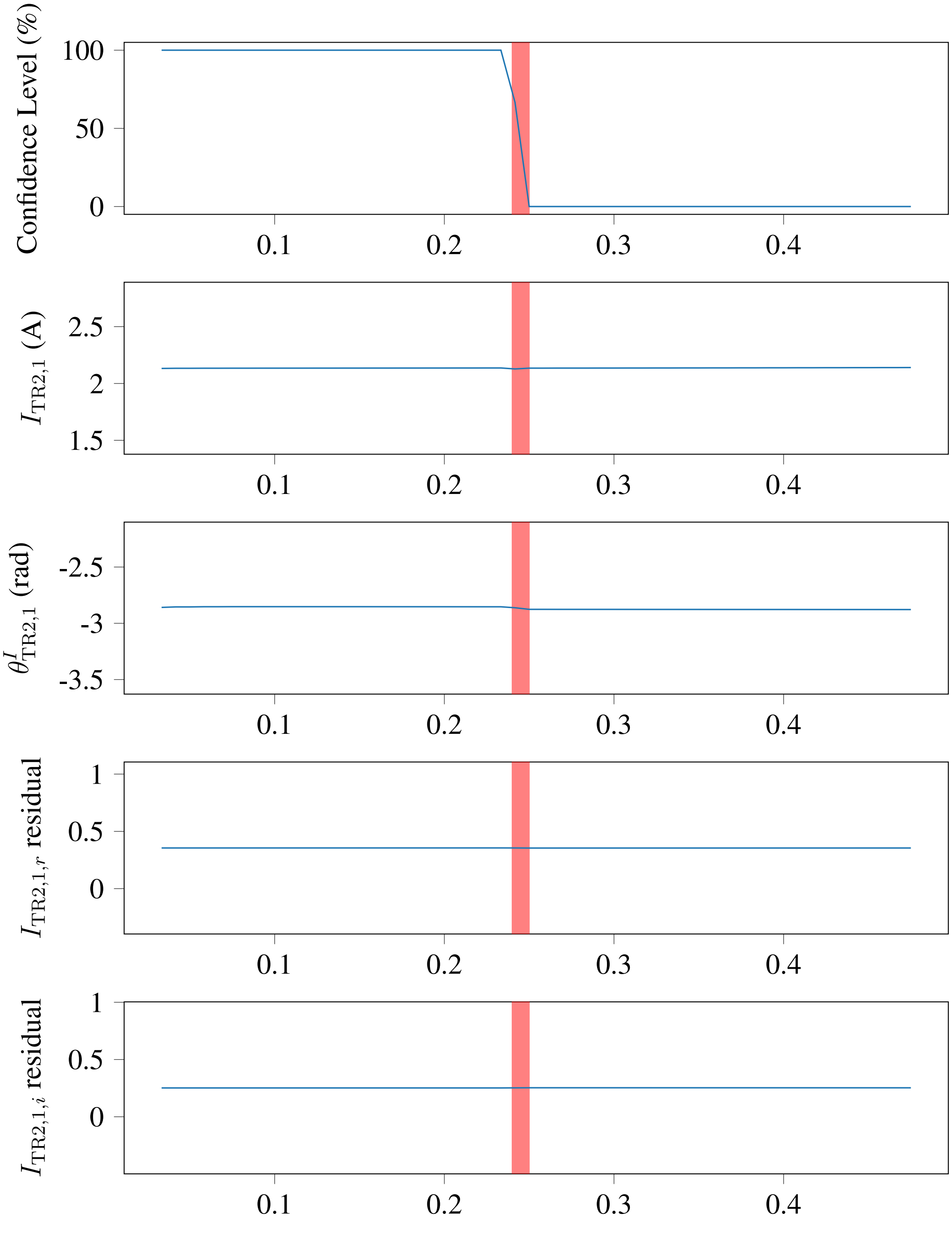

Figure 7.27: Microgrid confidence level, $i_{\mathrm{TR2,1}}$ measurements, and corresponding absolute normalized residuals (without hypothesis testing).

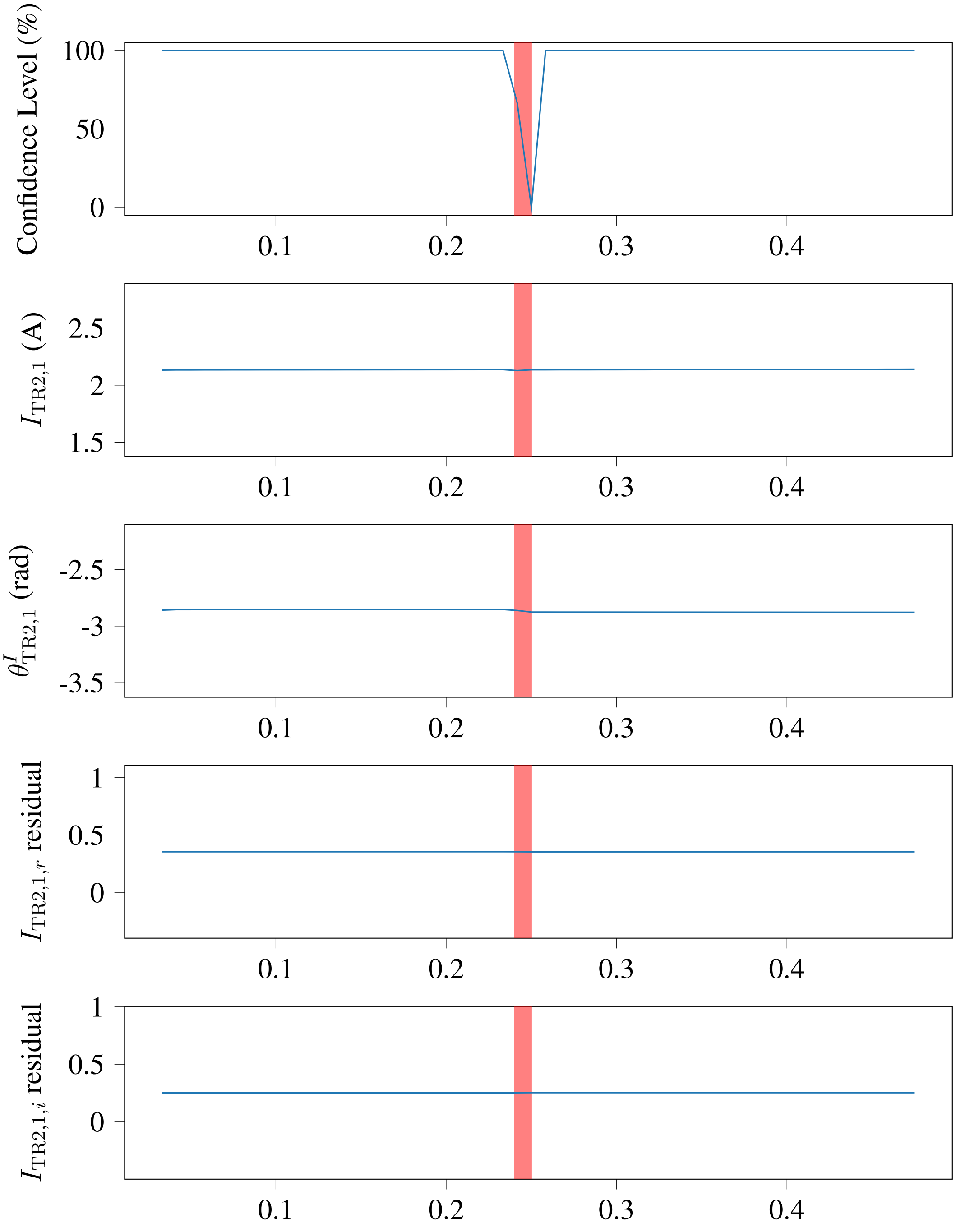

Figure 7.28: Microgrid confidence level, $i_{\text{TR2,1}}$ measurements, and corresponding absolute normalized residuals (with hypothesis testing).

7.2.1 Microgrid Schematic and Description

As was the case with the simplified microgrid of the previous section, the microgrid of this section is simulated in the WinIGS software. A screenshot of the microgrid captured in WinIGS is provided in Figure 7.29, and in magnified form in Figures 7.30 to 7.32. In the provided screenshots the microgrid is connected to a simplified equivalent of the power grid through a transformer.

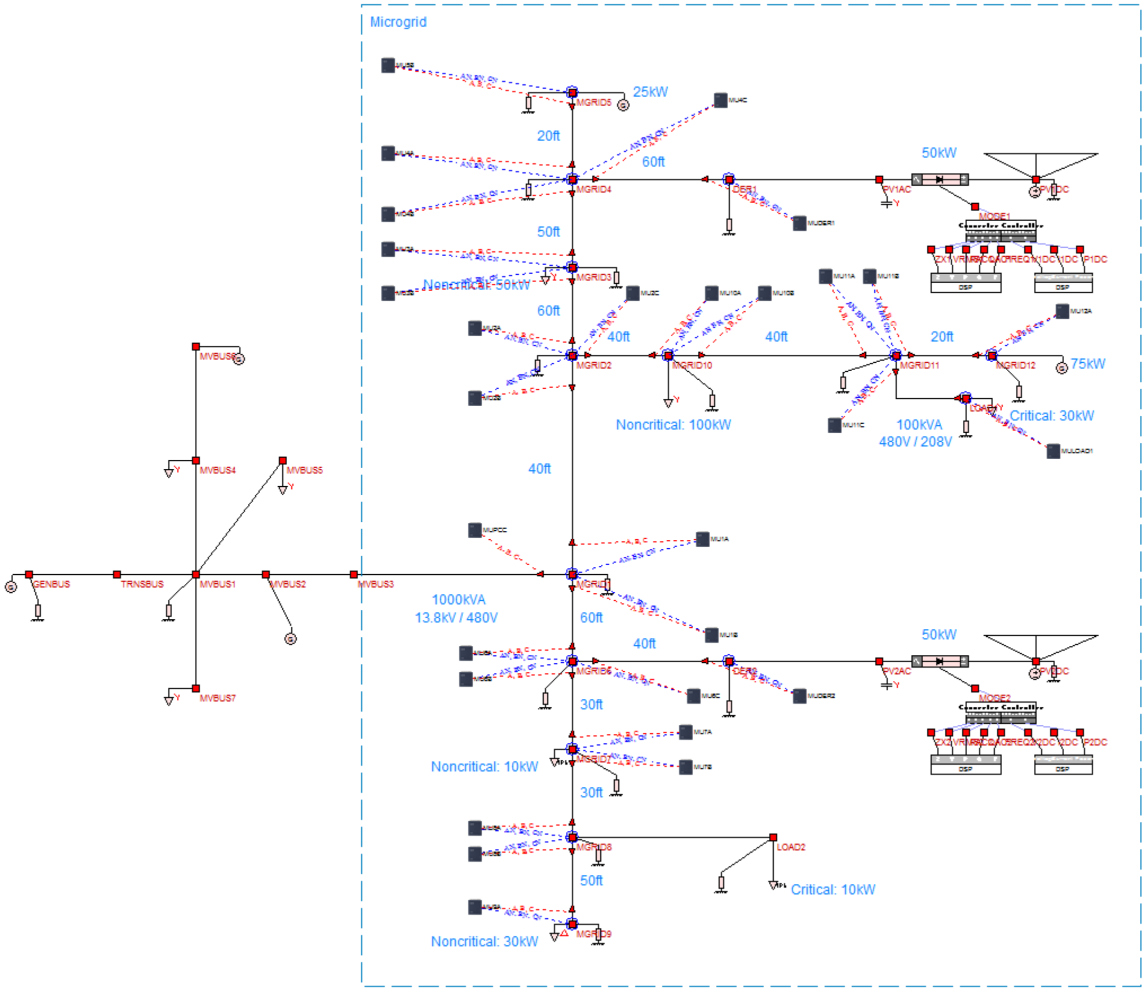

Figure 7.29: Detailed test system.

Once more, the power grid is modeled with an equivalent representation for generation and transmission connected to the distribution system through a which is connected to the distribution system through a 100 MVA, 115 kV/13.8 kV three-phase transformer in a delta-

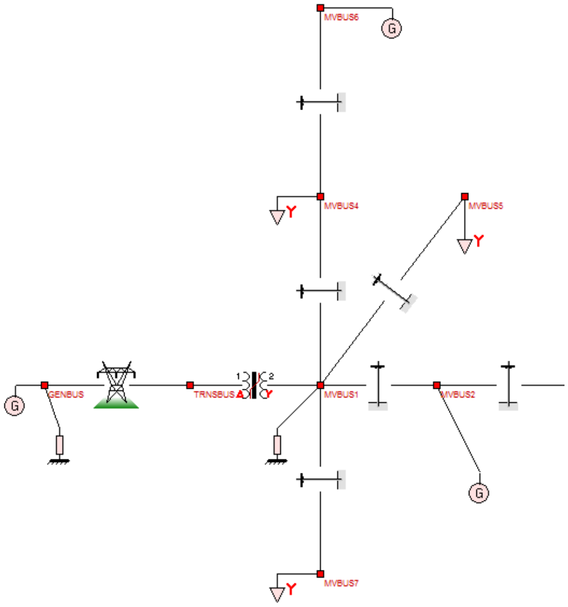

Figure 7.30: Magnified view: Left portion of the detailed test system.

wye configuration with grounded wye. The distribution system provides service to three 8 MW three-phase loads, as well as two 10 MVA distributed generators and the microgrid under study.

The microgrid is connected to the rest of the grid with a 1000 kVA, 13.8 kV/480 V three-phase transformer between buses MVBUS3 and MGRID1 in a delta-wye configuration with grounded wye. The microgrid loads are categorized into critical (one three-phase and one single-phase loads) and noncritical (three three-phase and one single-phase loads) for a total of four three-phase and two single-phase loads. The microgrid generation comprises two identical batteries modeled as DC sources interfaced with DC/AC inverters and controlled with Sinusoidal Pulse Width Modulation (SPWM), and two distributed generators. The microgrid buses are connected with 600 V copper cables of various lengths between 20 ft and 60 ft. There are 13 such cables in total. Moreover, there are two transformers within the microgrid, and a total of 16 buses. A summary is provided in Tables 7.4 to 7.6.

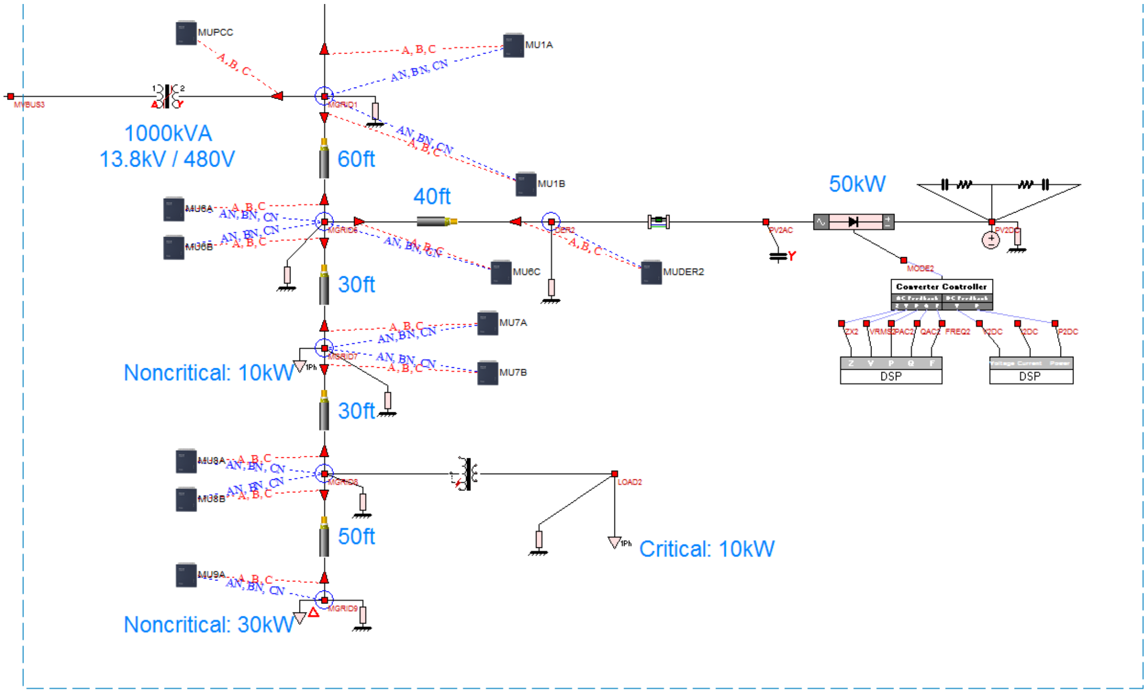

Figure 7.31: Magnified view: Lower right portion of the detailed test system.

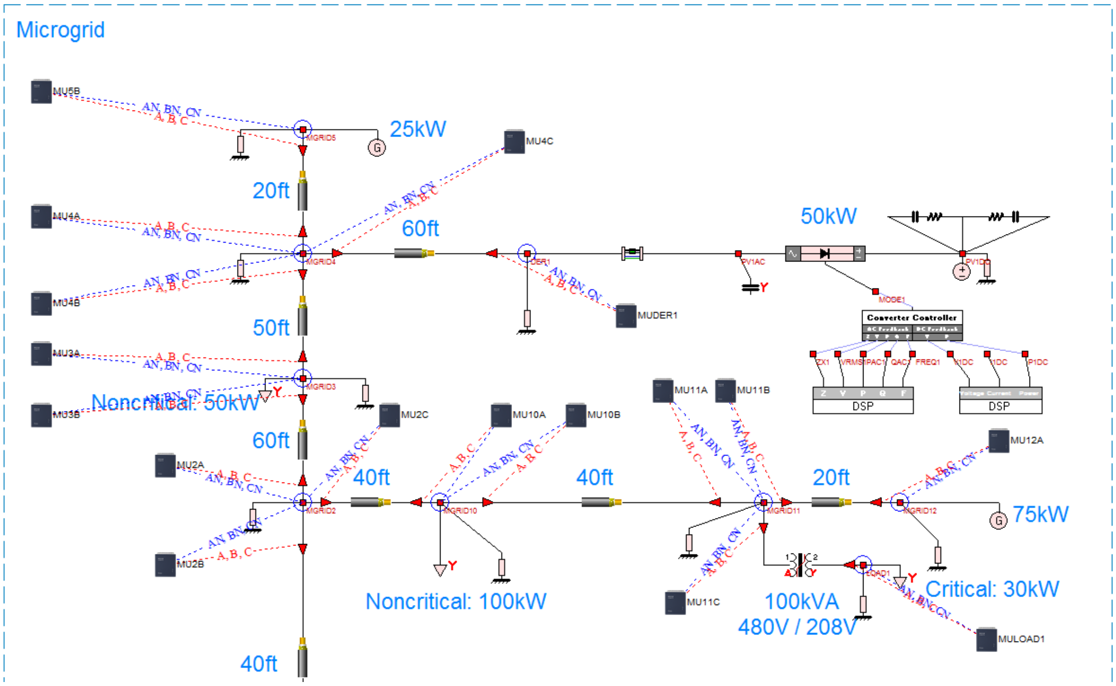

Figure 7.32: Magnified view: Upper right portion of the detailed test system.

Table 7.4: Second Microgrid Test System: Distributed Generation

Bus	Type	Nominal Voltage	Nominal Power
MGRID5	Generator	480 V	25 kW
MGRID12	Generator	480 V	75 kW
DER1	Battery Array	480 V	50 kW
DER2	Battery Array	480 V	50 kW

Table 7.5: Second Microgrid Test System: Load

Bus	Type	Nominal Voltage	Nominal Power
MGRID3	Noncritical 3-phase	480 V	50 kW
MGRID7	Noncritical 1-phase	480 V	10 kW
MGRID9	Noncritical 3-phase	480 V	30 kW
MGRID10	Noncritical 3-phase	480 V	100 kW
LOAD1	Critical 3-phase	208 V	30 kW
LOAD2	Critical 1-phase	240 V	10 kW

The detailed microgrid of this example is monitored by a total of 29 IEDs. One of them monitors the three currents at the interface of the microgrid with the rest of the grid. Each of the remaining IEDs monitors three voltages and three currents within the microgrid. Therefore, there are 171 monitored quantities. Again, due to the usage of phasors for the proposed protection scheme, a total of 342 actual measurement streams are used. Actual measurements are augmented with virtual and pseudo measurements. Here, there are 16 complex pseudo measurements; one at each microgrid bus. Therefore, the total number of pseudo measurements is 32. Within the monitored protection zones there is only one device whose model in the quasi-dynamic domain may contain virtual equations, namely the transformer between the MGRID11 and LOAD1 buses. Transformers like this can be accurately modeled with three internal equations, so six total virtual measurements are added to the measurement model. Hence, the measurement model contains a measurement total n_z equal to 380. A summary is provided in Table 7.7.

As far as states are concerned, there are 13 protection zones covering cables, each with six complex states, while the transformer model contains ten complex states, seven of which describe terminal voltages and three of which are internal state variables. Therefore,

Table 7.6: Second Microgrid Test System: Transformers

From	To	Nominal Voltage	Nominal Power
MGRID11	LOAD1	480 V/208 V	100 kVA
MGRID8	LOAD2	277 V/240 V	15 kVA

Table 7.7: Second Microgrid Test System: Total Measurements

Measurement Type	Total Number
Actual	342
Derived	0
Virtual	6
Pseudo	32
Total (n_z)	380

there is a total of 88 complex state variables, so the total number of states n_x within the microgrid studied here is 176. This means that the redundancy coefficient R_c equals 2.159 in this example.

7.2.2 Protection Zone Schematic and Description

For the remainder of this example, emphasis will be placed on a specific protection zone, in order to make comparisons easier. The selected protection zone contains the cable connecting MGRID3 to MGRID4. A closer view is provided in Figure 7.33.

The cable contains three conductors; one for each phase. Here, the protection zone voltages for each phase are named after their corresponding bus, and the protection zone currents for each phase are named after the bus from which the current is leaving.

The voltages recorded on the MGRID3 side of the cable are $v_{\mathrm{MGRID3,A}}$, $v_{\mathrm{MGRID3,B}}$, and $v_{\mathrm{MGRID3,C}}$, while the recorded currents are $i_{\mathrm{MGRID3,A}}$, $i_{\mathrm{MGRID3,B}}$, and $i_{\mathrm{MGRID3,C}}$, respectively. The primary measurements for these quantities are taken by the MU3A IED. Moreover, the MU3B IED contributes the secondary voltage measurements $v'_{\mathrm{MGRID3,A}}$, $v'_{\mathrm{MGRID3,B}}$, and $v'_{\mathrm{MGRID3,C}}$. It should be noted that due to the presence of a load connected to the MGRID3 bus, the currents recorded by MU3B cannot serve as secondary measurements for the currents recorded by MU3A.

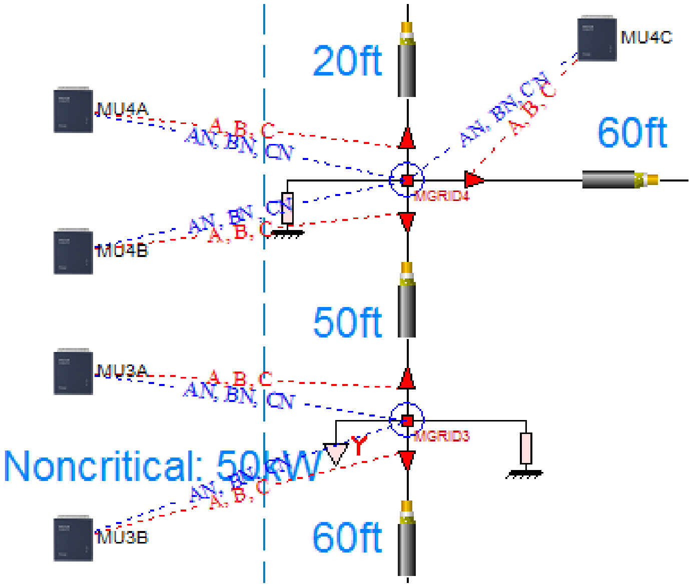

Figure 7.33: Protection zone schematic.

On the other side of the cable, the MU4B IED records three voltages and three currents, namely $v_{\text{MGRID4,A}}$, $v_{\text{MGRID4,B}}$, $v_{\text{MGRID4,C}}$, $i_{\text{MGRID4,A}}$, $i_{\text{MGRID4,B}}$, and $i_{\text{MGRID4,C}}$. Secondary measurements for the currents recorded by MU4B can be calculated using KCL with the currents recorded by MU4A and MU4C, as the sum of these currents should be equal and opposite to the currents recorded by MU4B for respective phases. Thus, measurements $i'_{\text{MGRID4,A}}$, $i'_{\text{MGRID4,B}}$, and $i'_{\text{MGRID4,C}}$ are obtained. The existence of these measurements is a good demonstration of how the concept of derived measurements helps provide redundancy to the novel centralized protection scheme. Moreover, secondary voltage measurements $v'_{\text{MGRID4,A}}$, $v'_{\text{MGRID4,B}}$, and $v'_{\text{MGRID4,C}}$ can be obtained from either MU4A or MU4C. Here, the MU4A measurements are used without loss of generality, since they are practically identical with the MU4C voltage measurements. Table 7.8 summarizes the relationships between actual measurements and IEDs.

Each of the 21 time domain measurements of Table 7.8 is converted to phasor form before it can be used by the proposed protection scheme. Thus, a total of 42 actual and derived measurements are monitored for the cable protection zone of this example. Once more, internal calculations are performed using the rectangular representation of phasors.

Table 7.8: Second Microgrid Test System: Measurements and IEDs

Measurements	IEDs
$v_{\text{MGRID3,A}}$, $v_{\text{MGRID3,B}}$, $v_{\text{MGRID3,C}}$	MU3A
$i_{\text{MGRID3,A}}$, $i_{\text{MGRID3,B}}$, $i_{\text{MGRID3,C}}$	MU3A
$v'_{\text{MGRID3,A}}$, $v'_{\text{MGRID3,B}}$, $v'_{\text{MGRID3,C}}$	MU3B
$v_{\text{MGRID4,A}}$, $v_{\text{MGRID4,B}}$, $v_{\text{MGRID4,C}}$	MU4B
$i_{\text{MGRID4,A}}$, $i_{\text{MGRID4,B}}$, $i_{\text{MGRID4,C}}$	MU4B
$v'_{\text{MGRID4,A}}$, $v'_{\text{MGRID4,B}}$, $v'_{\text{MGRID4,C}}$	MU4A
$i'_{\text{MGRID4,A}}$, $i'_{\text{MGRID4,B}}$, $i'_{\text{MGRID4,C}}$	MU4A & MU4C

The cable model does not contain any virtual equations, so no virtual measurements are considered here. However, there exist two complex (or four real) pseudo measurements due to the neutrals at buses MGRID3 and MGRID4. Therefore, the total number of monitored measurements n_z is 46. The cable model here uses six complex state variables. Therefore, the total number of states n_x within the protection zone under study is 12, which means that the redundancy coefficient R_c is approximately 3.83 for this zone.

Finally, it should be noted that for the rest of this example, each IED is treated as an independent instrumentation channel with the exception of MU4A and MU4C, which are considered as a single instrumentation channel, because they need to combine for the secondary MGRID4 current measurements. This means that here, unlike the previous example, multiple measurements will be treated as one group for elimination purposes.

7.2.3 Compromised Data

Attack and recorded waveforms

The first scenario to be tested on the detailed microgrid is an attack on the MU4B IED. It is assumed that an attacker successfully manages to get access to this specific IED and imitate a three-phase-to-ground fault on the cable connecting bus MGRID4 to bus MGRID3. In that case, the MU4B IED would record a voltage drop at MGRID4 and an increase in the currents flowing towards MGRID3.

Such a combination of events should trigger the protection of the affected cable. A legacy undervoltage protection scheme could have been triggered by the voltage drop, and a legacy differential protection scheme that would calculate the mismatch between the currents flowing through the cable should have also tripped the breakers of the affected zone.

Here, it is assumed that at the time of the attack voltage measurements $v_{\text{MGRID4,A}}$, $v_{\text{MGRID4,B}}$ and $v_{\text{MGRID4,C}}$ drop by 50%, and currents $i_{\text{MGRID4,A}}$, $i_{\text{MGRID4,B}}$ and $i_{\text{MGRID4,C}}$ appear to be five times larger. The time of the attack is set at 200 ms.

Any relay monitoring the attacked protection zone will have access to the measurements from MU3A and MU4B. These are provided in Figures 7.34 to 7.37. Apart from the effect of the attack, it is also worth noting that the recorded waveforms are somewhat distorted due to harmonic content introduced by the explicit modeling of the power electronics of the two inverter-interfaced DERs as well as their corresponding controllers.

The waveforms in Figures 7.34 to 7.37 exhibit sufficiently abnormal behavior to trigger any properly designed protection scheme responsible for this specific protection zone, including settingless relays. For example, legacy differential protection schemes are programmed to observe that the currents at the two endpoints of each phase are very far from being equal and opposite, thus concluding that a fault has occurred. Any individual zone protection relay that detects such a fault in the cable between buses MGRID3 and MGRID4 reacts by disconnecting the cable to avoid further harm to any bystander or piece of equipment. If such an action is indeed undertaken, it will at least lead to the loss of the distributed generation at buses MGRID5 and DER1. Therefore, the operation of the microgrid will be severely compromised. The protection scheme that is introduced in this thesis is designed to supervise the individual protection zone relays and avert such a catastrophic scenario.

In this example, the introduced scheme provides protection against erroneous tripping once more through the combination of multiple measurement streams from both inside and outside the affected protection zone. For the measurement streams of Table 7.8, the calculated phasors for phase A quantities are provided in Figures 7.38 and 7.39. The reader may observe the attack by comparing the measurements streamed from the compromised

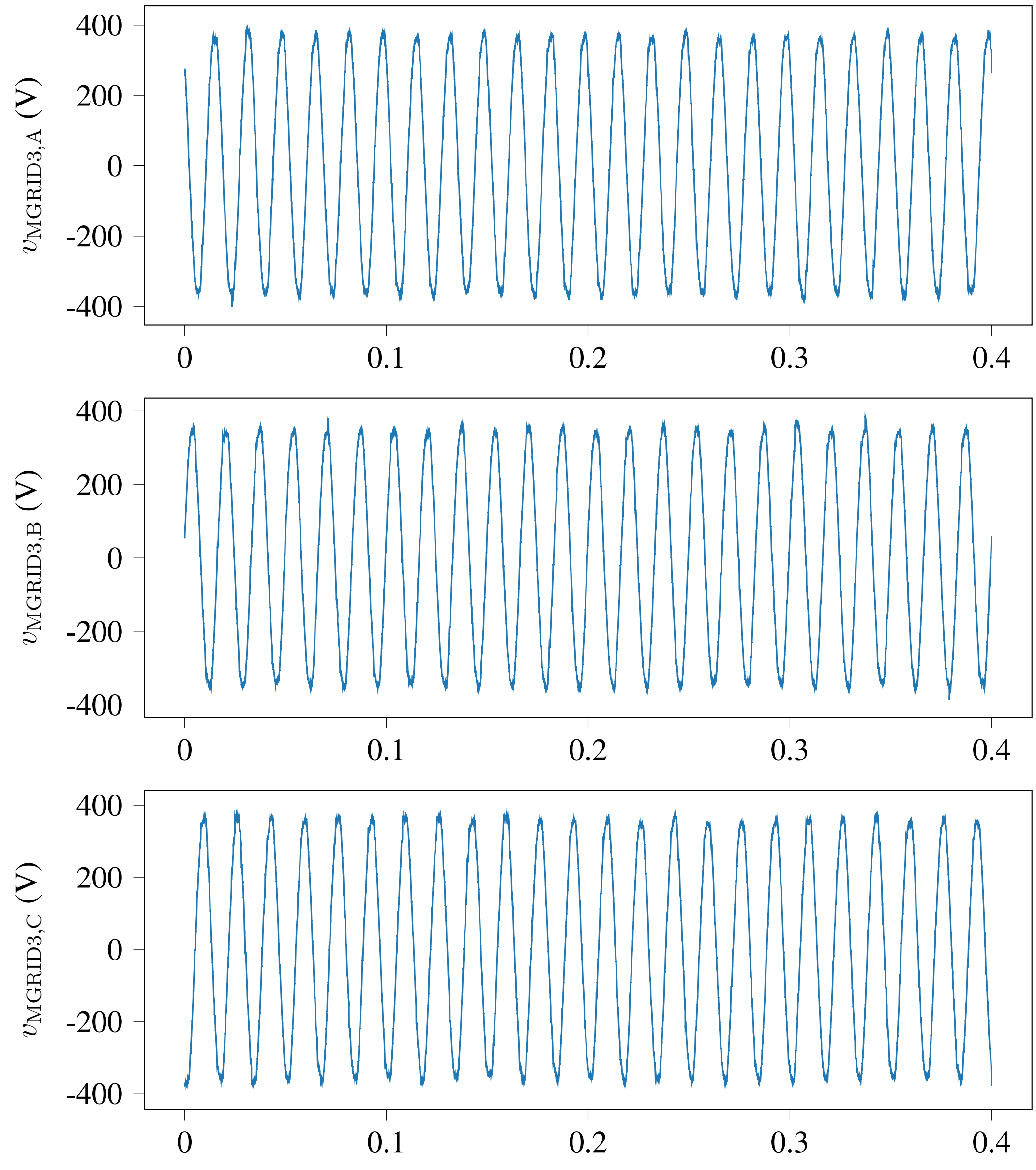

Figure 7.34: Voltage waveforms recorded by the MU3A IED.

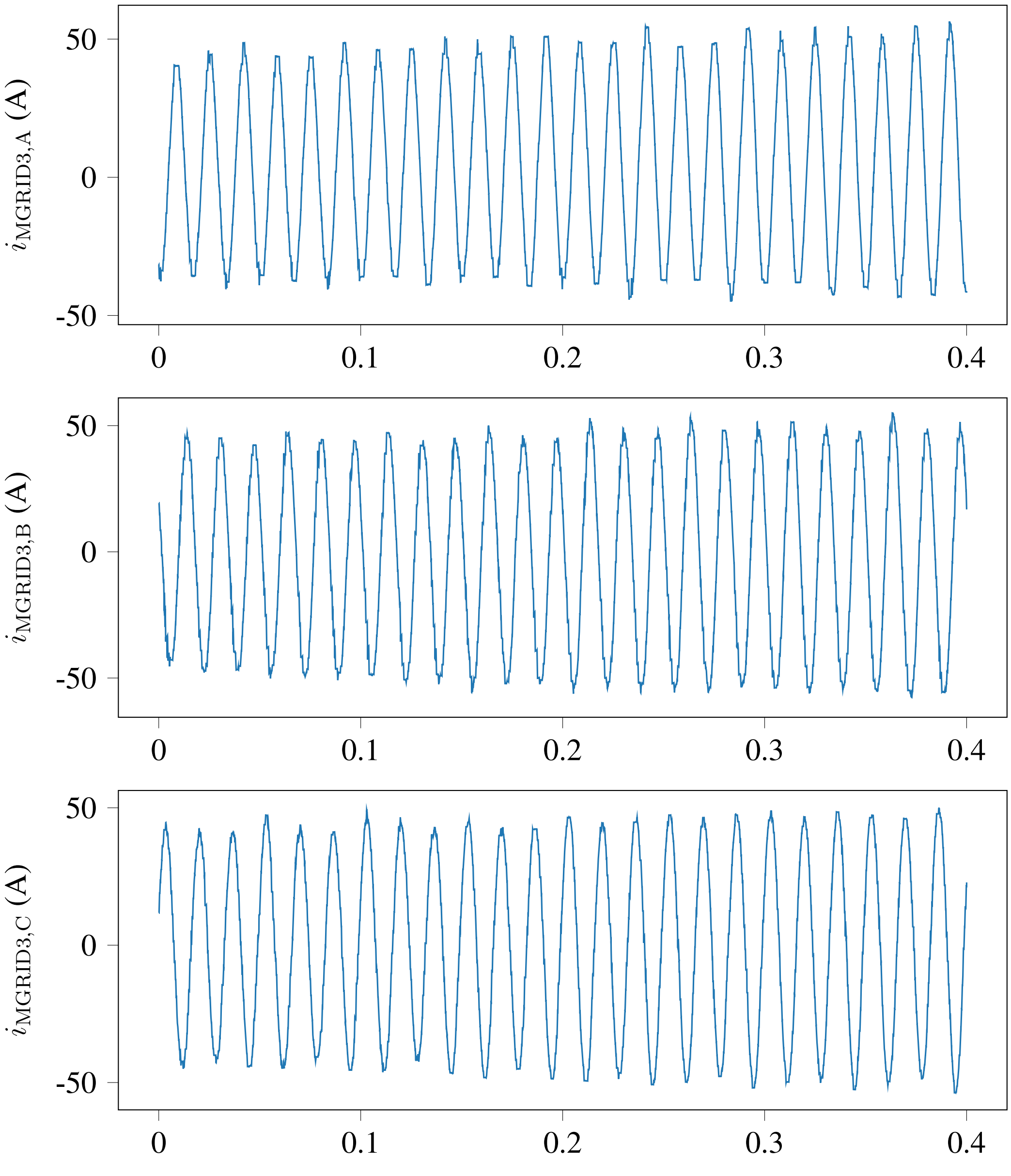

Figure 7.35: Current waveforms recorded by the MU3A IED.

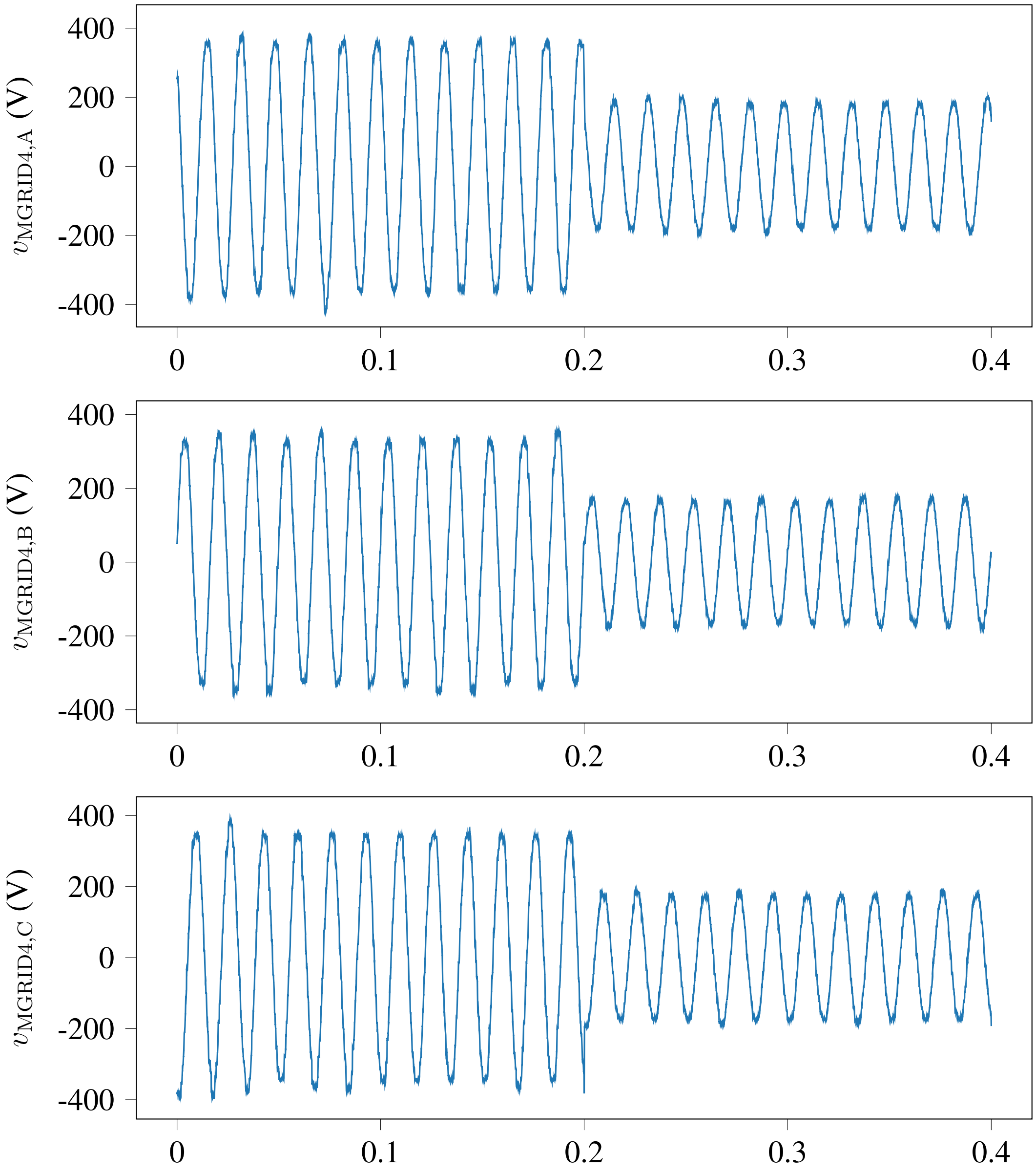

Figure 7.36: Voltage waveforms recorded by the MU4B IED.

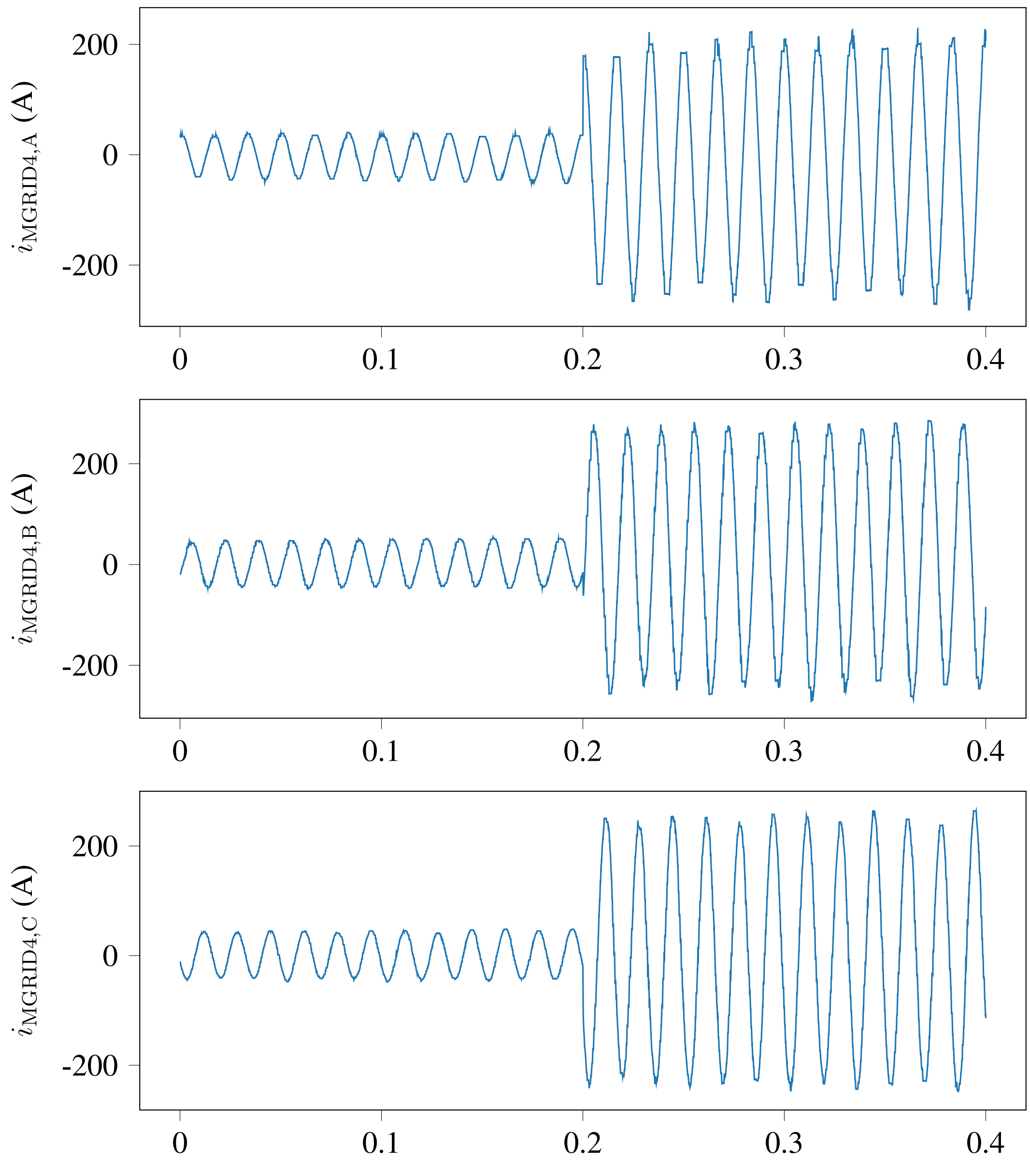

Figure 7.37: Current waveforms recorded by the MU4B IED.

MU4B IED with the redundant measurements of the same quantities streamed by IEDs MU4A and MU4C. The goal of the centralized protection scheme is to reach the same conclusion by analyzing the measurements it has at its disposal.

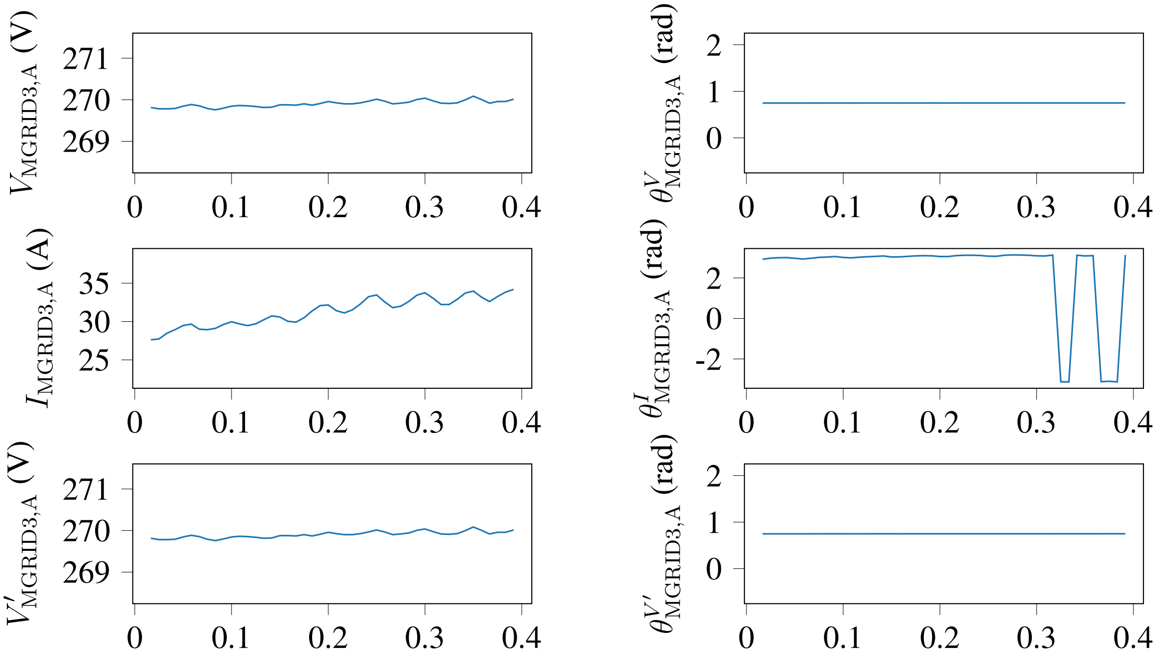

Figure 7.38: Calculated phasors for the MU3A IED.

Protection algorithm execution

The protection scheme operates in a way similar to the previous test case.

First, a microgrid measurement model can be obtained by following the object-oriented procedure that has already been presented in previous chapters. While the models employed here are more detailed when it comes to their power electronics, the same basic principles can be followed in an automated way to provide the measurement model.

Once more, the core of the protection scheme is the execution of DSE in the quasi-dynamic domain twice per cycle based on phasors calculated over a rolling window of one cycle.

Figure 7.40 shows the calculated confidence level, as well as the magnitude and angle

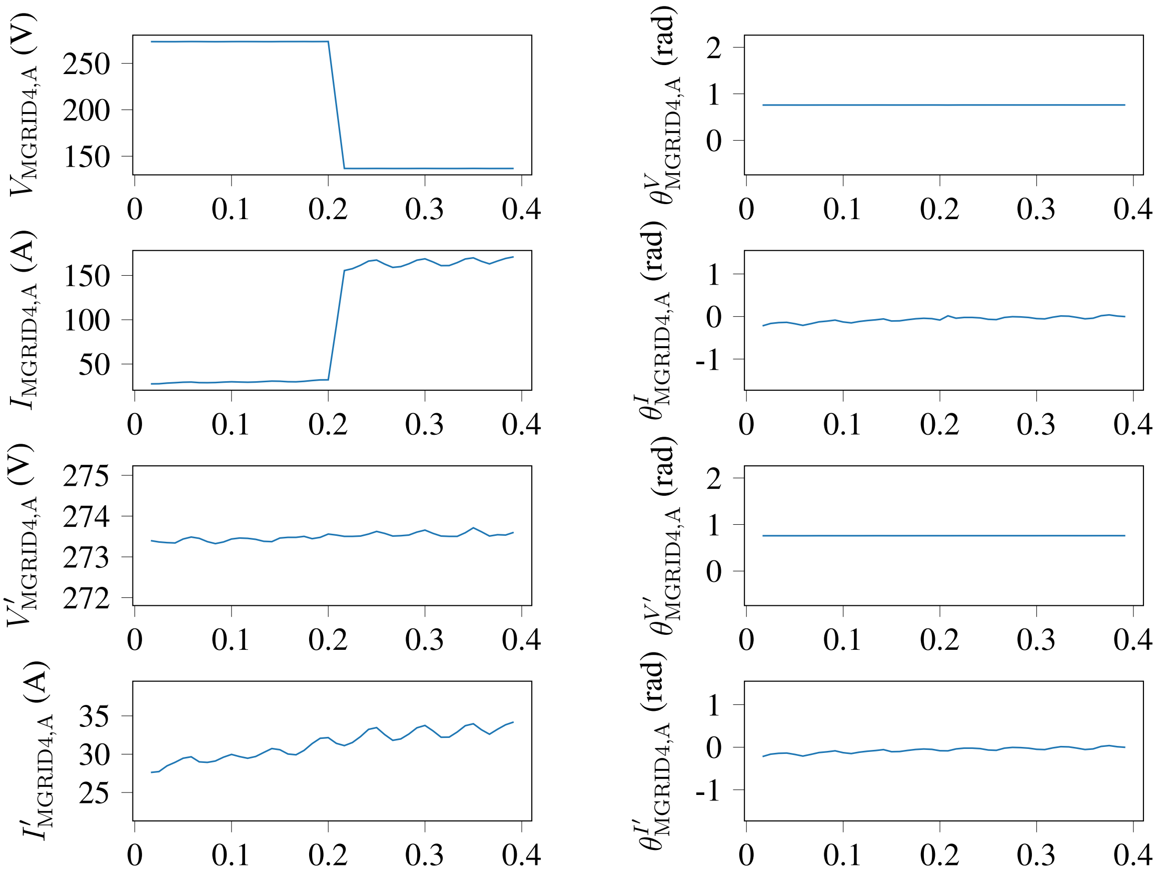

Figure 7.39: Calculated phasors for the MU4B IED.

measurements for the $i_{\text{MGRID4,B}}$ phasor, and the corresponding absolute normalized residuals for the real and imaginary parts of the phasor. It should be emphasized again that the internal calculations for the proposed centralized protection scheme are performed using rectangular coordinates, so the absolute normalized residuals correspond to rectangular quantities. In this figure, the internal calculations are performed with the hypothesis testing module deactivated for comparison purposes.

The values of the confidence level before the initiation of the attack are large as expected with the minimum being equal to 99.97%. Once the attack commences, the first execution of DSE finds a confidence level equal to 45.84%. This is well below any threshold c_t that has been used for testing purposes, as these usually range between 50% and 80%. One DSE step later and the confidence level dropped below 1%, which is a good indicator of

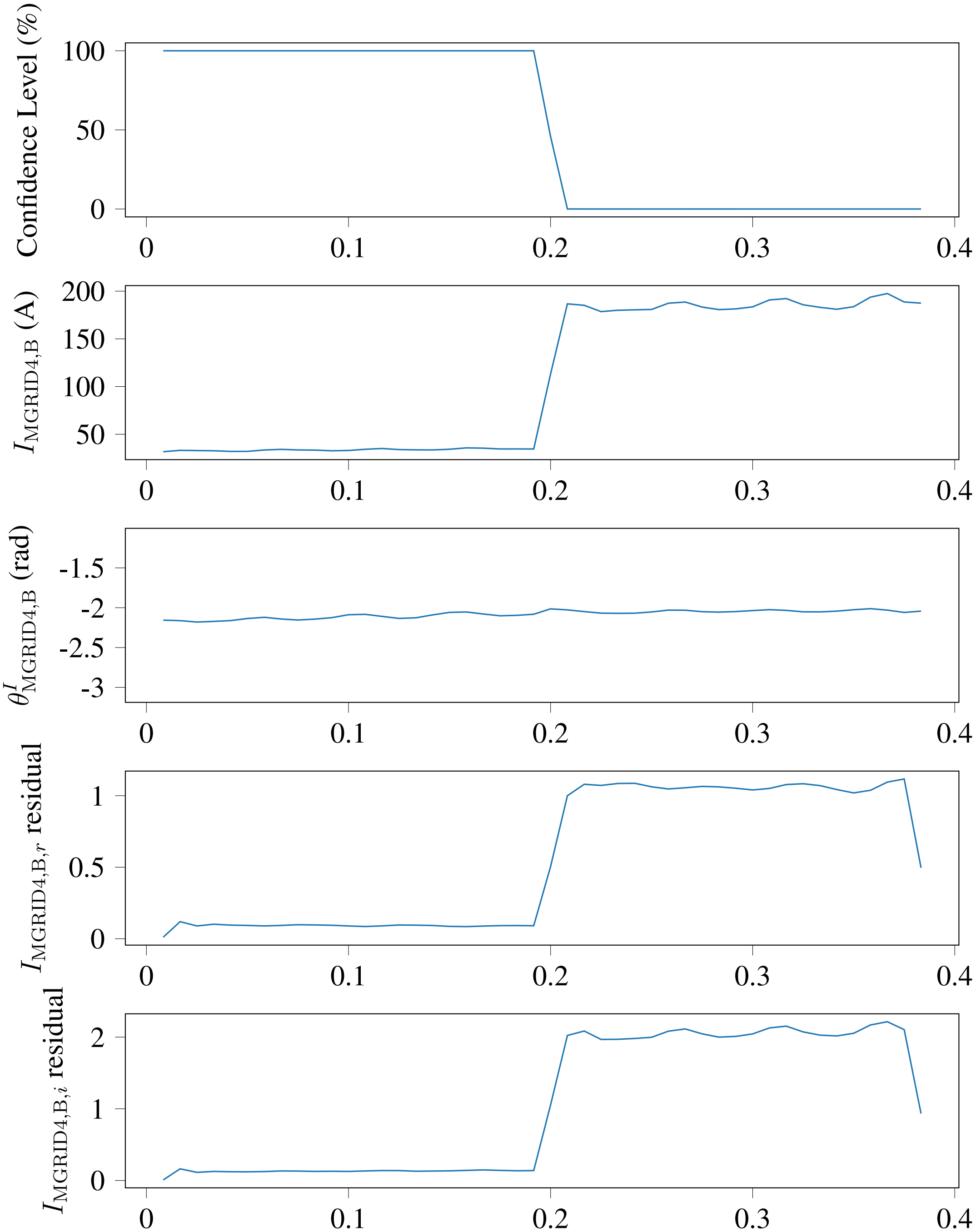

Figure 7.40: Microgrid confidence level, $i_{\mathrm{MGRID4,B}}$ measurements, and corresponding absolute normalized residuals (without hypothesis testing).

abnormal conditions. It is worth noting how abruptly the confidence level changed within just two DSE execution steps once the attack was initiated.

As the confidence level now indicates that there is an abnormality within the system, the hypothesis testing module needs to be executed. This module utilizes the value of the absolute normalized residual r_n for each measurement. The ten largest absolute normalized residuals are presented in Table 7.9 alongside the corresponding measurements and instrumentation channels.

Table 7.9: Second Microgrid Test System: Suspect measurements under cyber-attack

r_n	Measurement	Instrumentation Channel
1.053	$i_{\mathrm{MGRID4,B}}$	MU4B
0.946	$i_{\mathrm{MGRID4,A}}$	MU4B
0.915	$i_{\mathrm{MGRID4,C}}$	MU4B
0.819	$v'_{\mathrm{MGRID3,C}}$	MU3B
0.771	$v'_{\mathrm{MGRID3,B}}$	MU3B
0.749	$i_{\mathrm{MGRID3,B}}$	MU3A
0.716	$i_{\mathrm{MGRID3,C}}$	MU3A
0.697	$i_{\mathrm{MGRID3,A}}$	MU3A
0.504	$i_{\mathrm{MGRID4,B}}$	MU4B
0.416	$i_{\mathrm{MGRID4,C}}$	MU4B

The following observations can be made based on Table 7.9. First, waveforms recorded by the attacked IED are indeed at the top of the list. Moreover, the largest measurement from MU4B, i.e., $i_{\mathrm{MGRID4,B}}$, is visibly larger than the largest measurement from any other IED, which proves to be a significant advantage of the proposed scheme once more. Furthermore, measurements $i_{\mathrm{MGRID4,B}}$ and $i_{\mathrm{MGRID4,C}}$ appear in this list twice, since each phasor corresponds to a real and an imaginary residual. Finally, since all measurements recorded by MU4B are grouped together and eliminated here, their relative order is not important. However, it does appear that in this case the protection scheme is more sensitive to current measurements compared to voltage measurements. This may be explained by noticing that the change in current magnitude after the attack is more significant than the change in voltage magnitude.

After the elimination of the six measurements streamed by MU4B the DSE procedure is repeated with the remaining measurements. Figure 7.41 shows the same quantities as Figure 7.40, but this time with the hypothesis testing and measurement elimination module activated.

The following observations can be made. First, the measurement elimination restored the confidence level to a normal value, thus verifying that the root cause of the drop is the detected IED. There is only one step with a low confidence level in this figure, namely the step where the confidence level dropped to 45.84%, thus triggering the hypothesis testing module. The next execution of the protection algorithm verifies the restoration of the confidence level to an acceptable range of values. This is achieved in the following way.

The hypothesis testing module removes the six measurements associated with the MU4B IED, namely $v_{\mathrm{MGRID4,A}}$, $v_{\mathrm{MGRID4,B}}$, $v_{\mathrm{MGRID4,C}}$, $i_{\mathrm{MGRID4,A}}$, $i_{\mathrm{MGRID4,B}}$, and $i_{\mathrm{MGRID4,C}}$. Once these measurements are eliminated, the microgrid measurement model needs to be updated. Then, DSE is performed with the new, reduced measurement model, and all relevant quantities, such as the normalized residuals and the confidence level, are calculated again. Since the removed measurements are not used anymore once the centralized protection scheme is activated, their normalized residuals are equal to zero for the rest of the interval, as is evident in Figure 7.41.

The confidence level restoration means that the system operator must be notified and any relay action must be prevented to avoid unnecessary (and harmful) tripping. As was the case in the previous example, the reaction time of the proposed scheme is very short, which is one of the main advantages of this protection method.

Figures 7.42 and 7.43 show the microgrid confidence level again, as well as the calculated phasor magnitude and angle, and calculated absolute normalized residuals in rectangular form for the $i_{\mathrm{MGRID4,C}}$ measurement, i.e., the measurement with the second highest normalized residual in Table 7.9. Once more, the reader can observe how the changes in this waveform after the initiation of the attack coincide with the confidence level drop and the rise in the value of the absolute normalized residuals corresponding to this measurement.

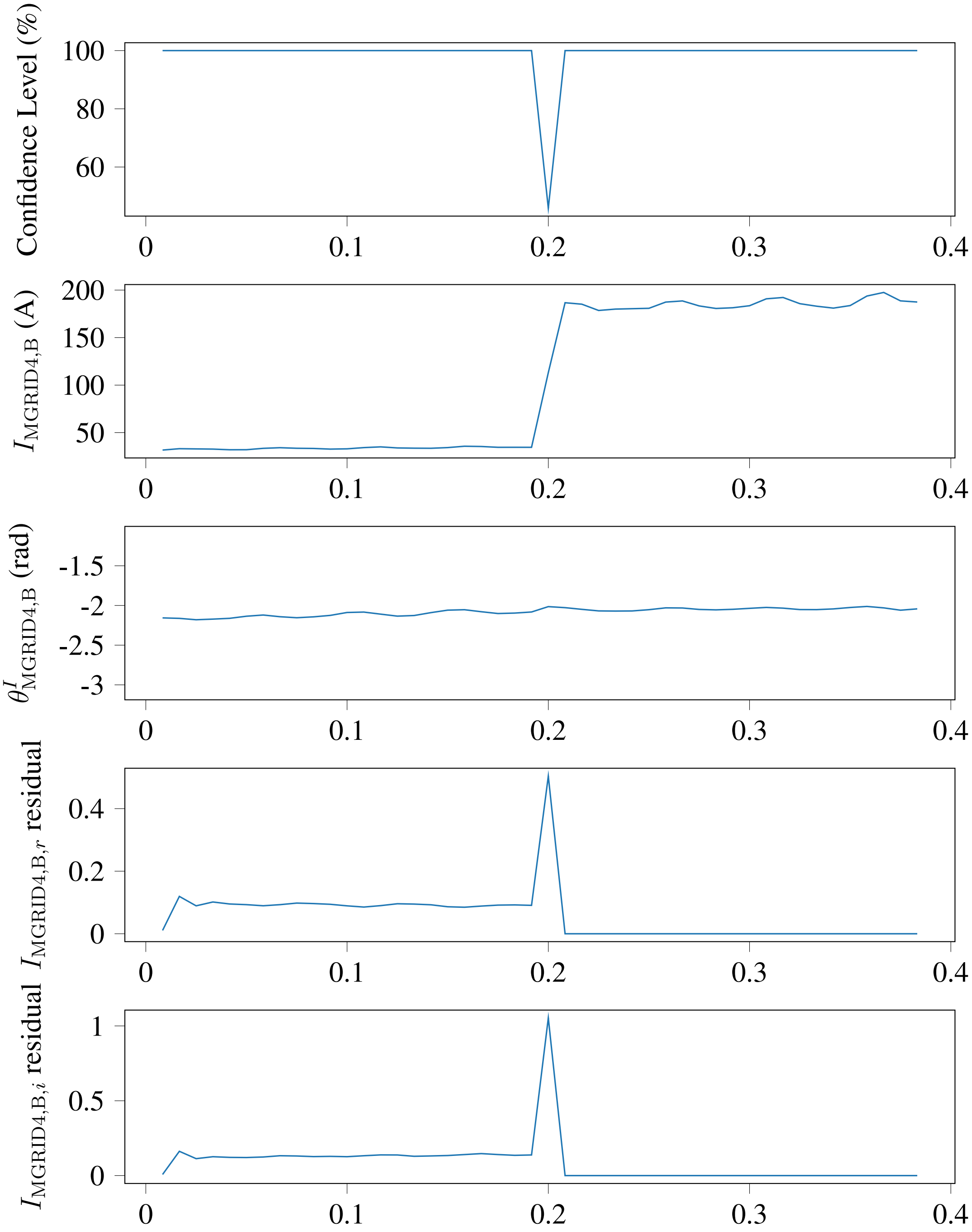

Figure 7.41: Microgrid confidence level, $i_{\mathrm{MGRID4,B}}$ measurements, and corresponding absolute normalized residuals (with hypothesis testing).

The removal of this measurement, since it is recorded by the same IED as the suspect measurement, can be also observed by the fact that the relevant absolute normalized residuals go to zero for the rest of the time window after the detection of the attack.

Among the voltage waveforms, $v'_{\mathrm{MGRID3,C}}$ is the one with the highest absolute normalized residual. Figures 7.44 and 7.45 show the microgrid confidence level again, as well as the calculated phasor magnitude and angle, and calculated absolute normalized residuals in rectangular form for the $v'_{\mathrm{MGRID3,C}}$ measurement. Incidentally, the $v'_{\mathrm{MGRID3,C}}$ waveform is recorded by the MU3B IED, which is not affected by the cyber-attack. Therefore, the hypothesis testing module should not remove this waveform. This is evident in Figure 7.45, as the corresponding absolute normalized residuals are not removed after the attack despite the operation of the hypothesis testing module.

7.2.4 Cable Fault

Power fault and recorded waveforms

In order to verify that the introduced protection scheme performs as expected in the presence of a power fault, the second scenario to be tested on the detailed microgrid is a ground fault affecting the cable connecting bus MGRID4 to bus MGRID3. The fault is set to start at 200 ms at the midpoint of the affected cable.

While a single-phase-to-ground fault is simulated here, the cable model includes the coupling between the conductors of the cable, so the fault will be visible in the recorded waveforms of all cable phases.

Any relay monitoring the cable between MGRID3 and MGRID4 will be receiving once more the twelve measurements recorded by MU3A and MU4B. These are provided in Figures 7.46 to 7.49.

As was the case with the cyber-attack on the detailed microgrid, the recorded waveforms exhibit some distortion due to the harmonic content caused by the existence of detailed models of DERs (and their controllers) within the studied microgrid.

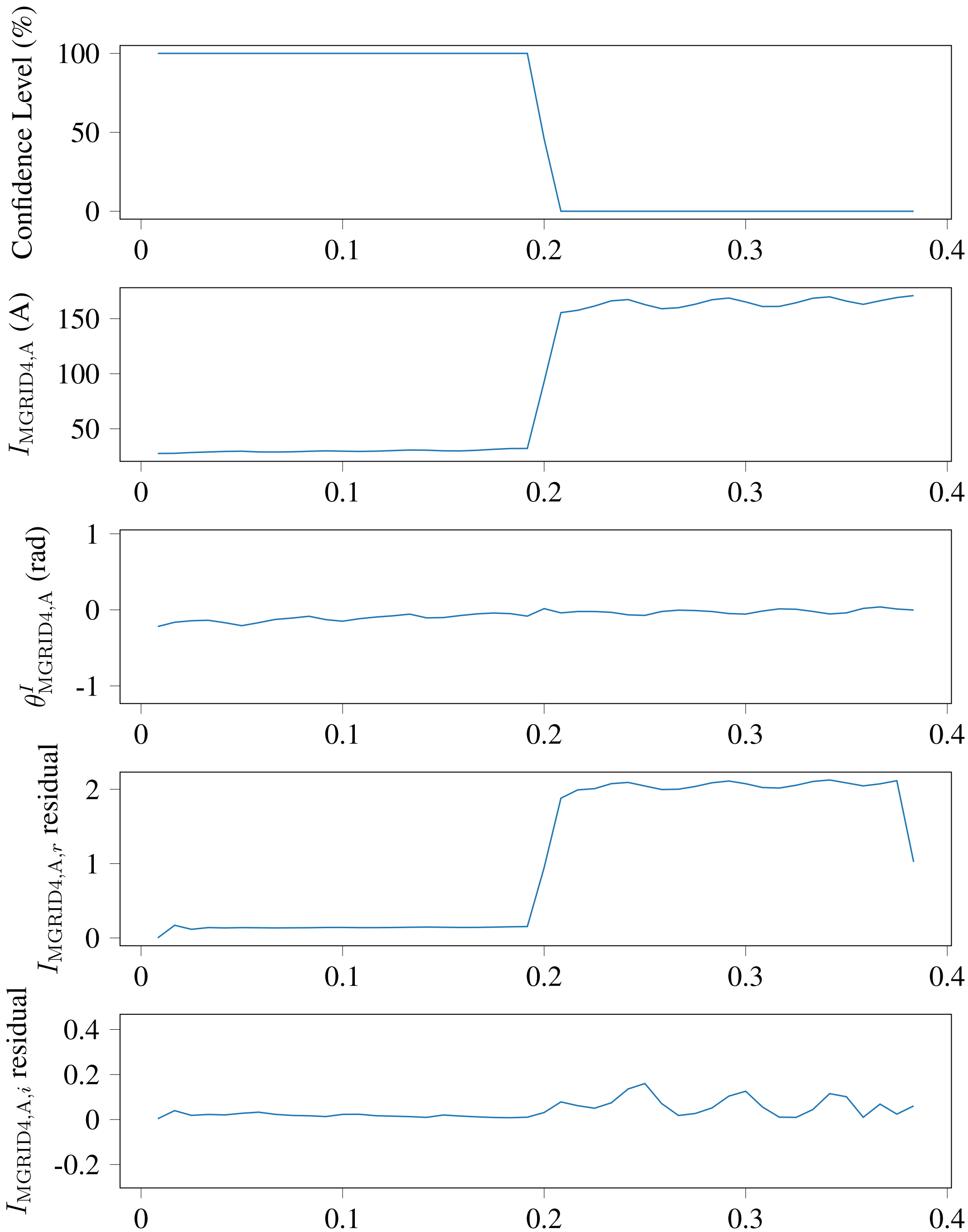

Figure 7.42: Microgrid confidence level, $i_{\mathrm{MGRID4,A}}$ measurements, and corresponding absolute normalized residuals (without hypothesis testing).

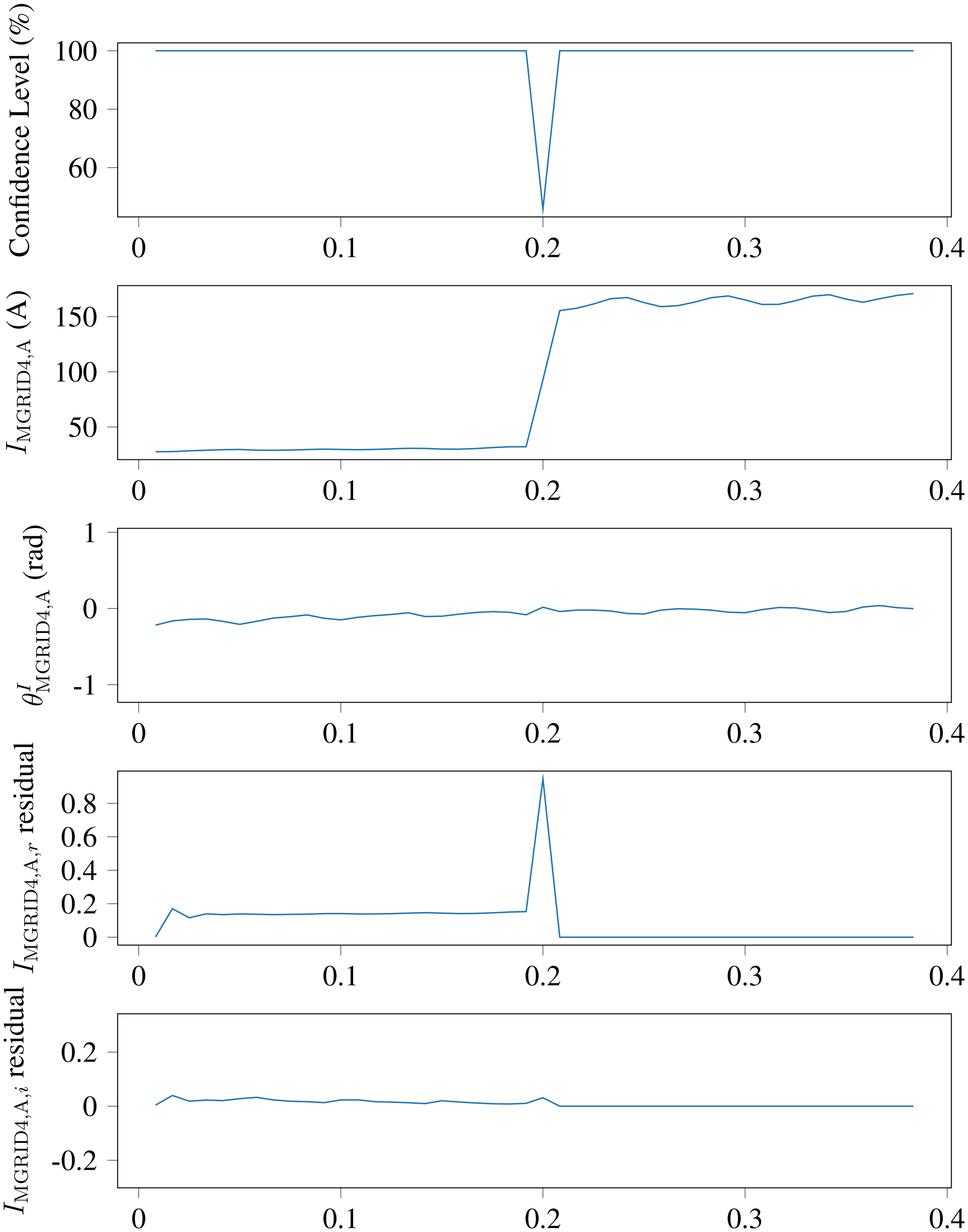

Figure 7.43: Microgrid confidence level, $i_{\text{MGRID4,A}}$ measurements, and corresponding absolute normalized residuals (with hypothesis testing).

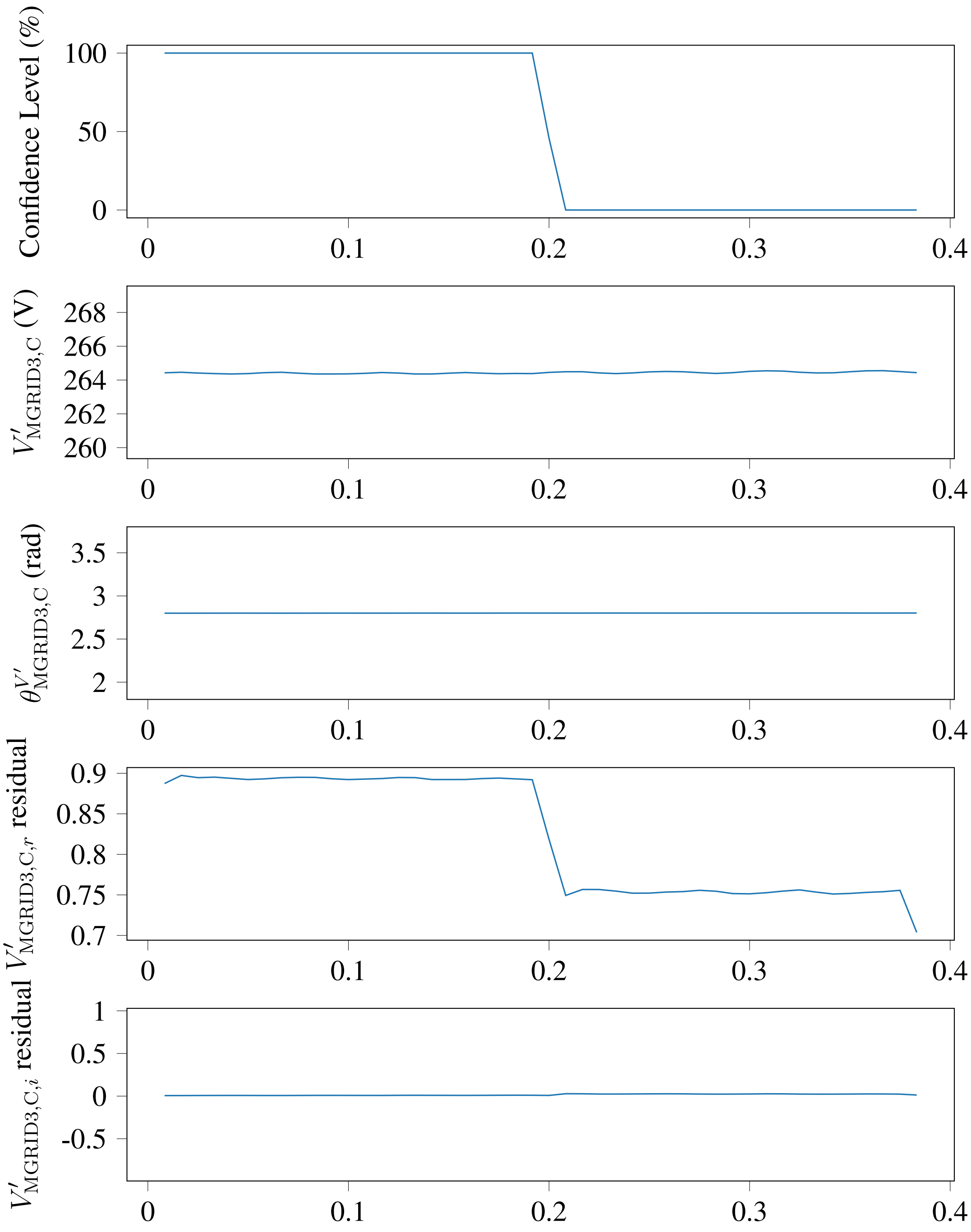

Figure 7.44: Microgrid confidence level, $v'_{\mathrm{MGRID3,C}}$ measurements, and corresponding absolute normalized residuals (without hypothesis testing).

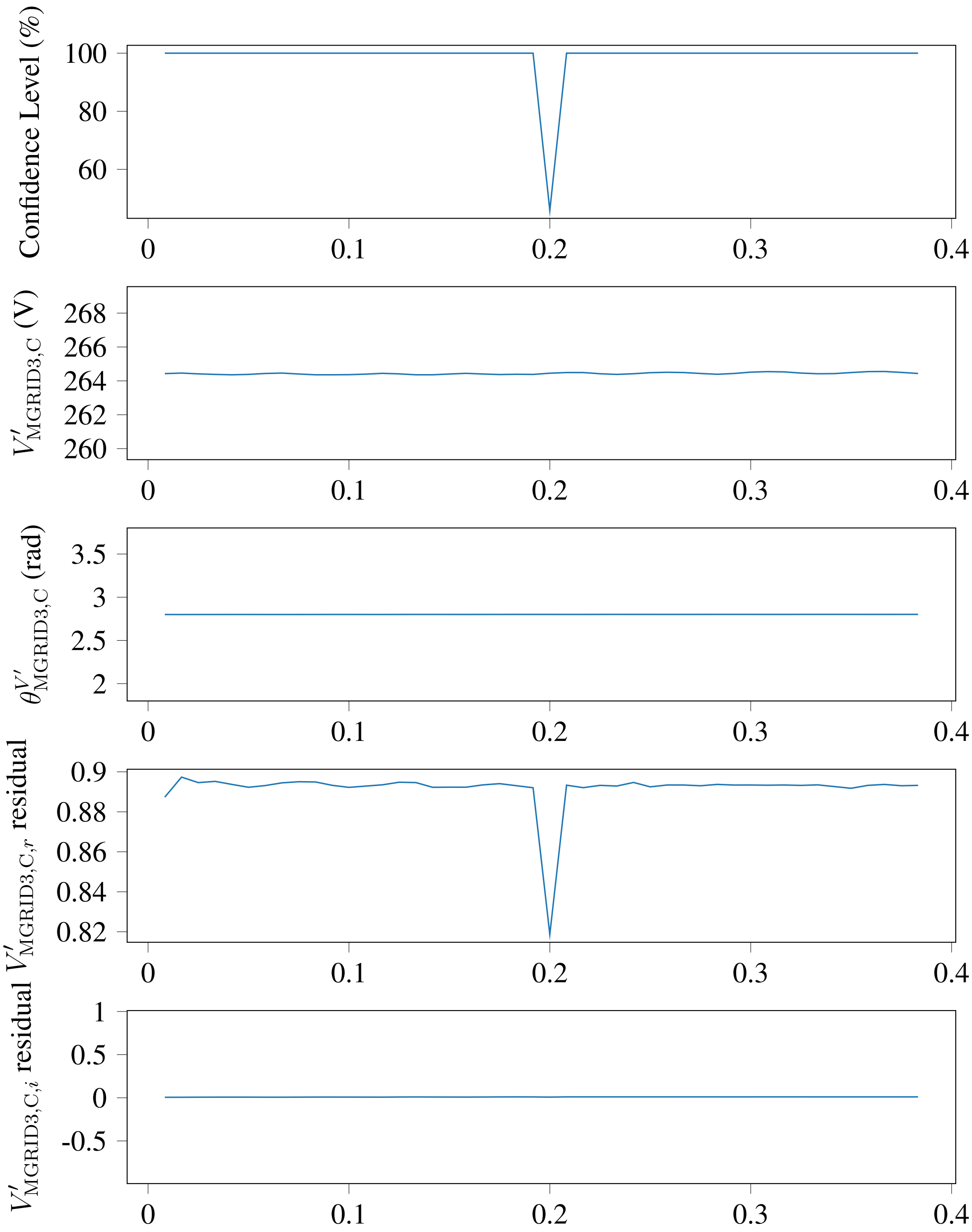

Figure 7.45: Microgrid confidence level, $v'_{\mathrm{MGRID3,C}}$ measurements, and corresponding absolute normalized residuals (with hypothesis testing).

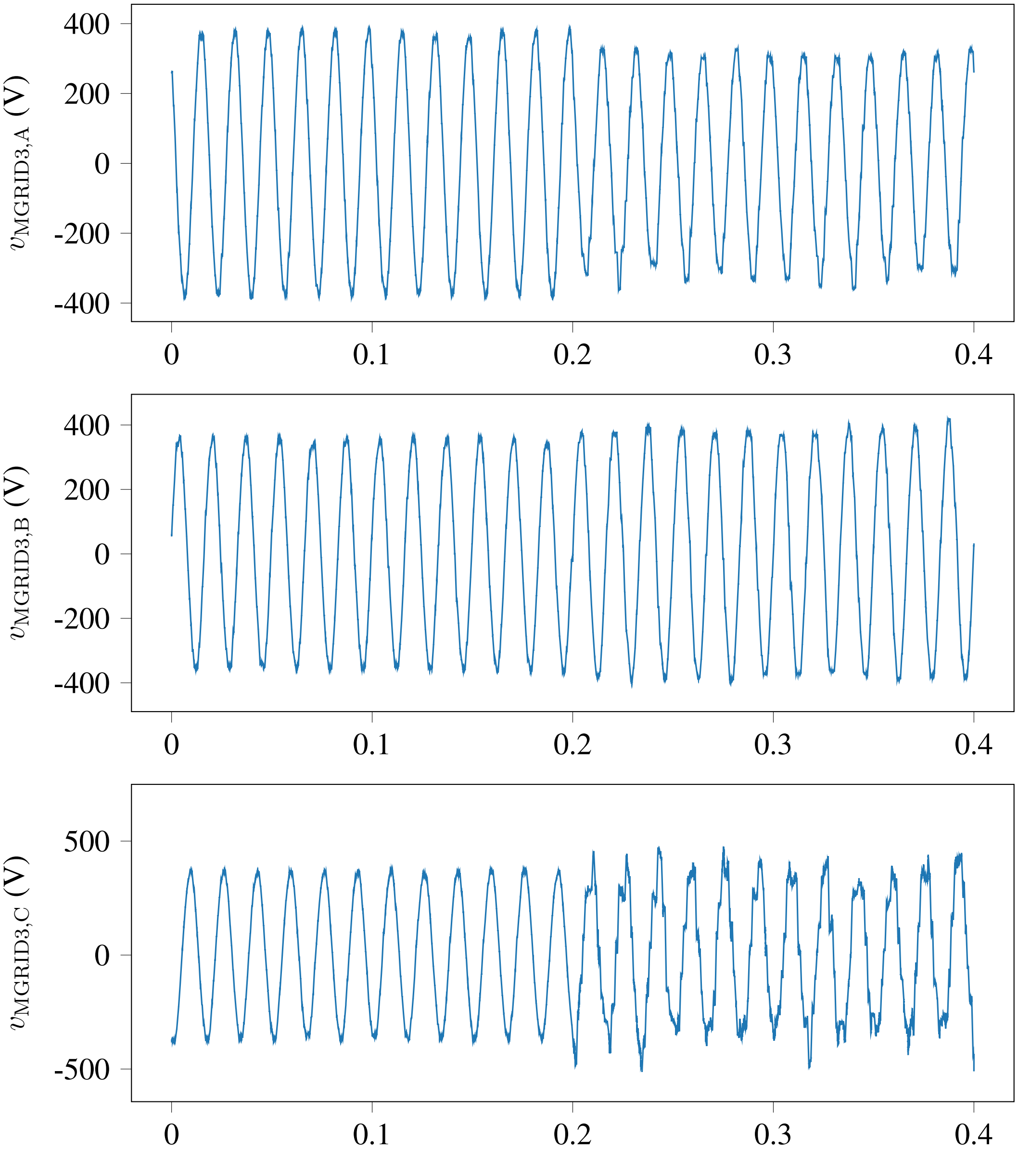

Figure 7.46: Voltage waveforms recorded by the MU3A IED.

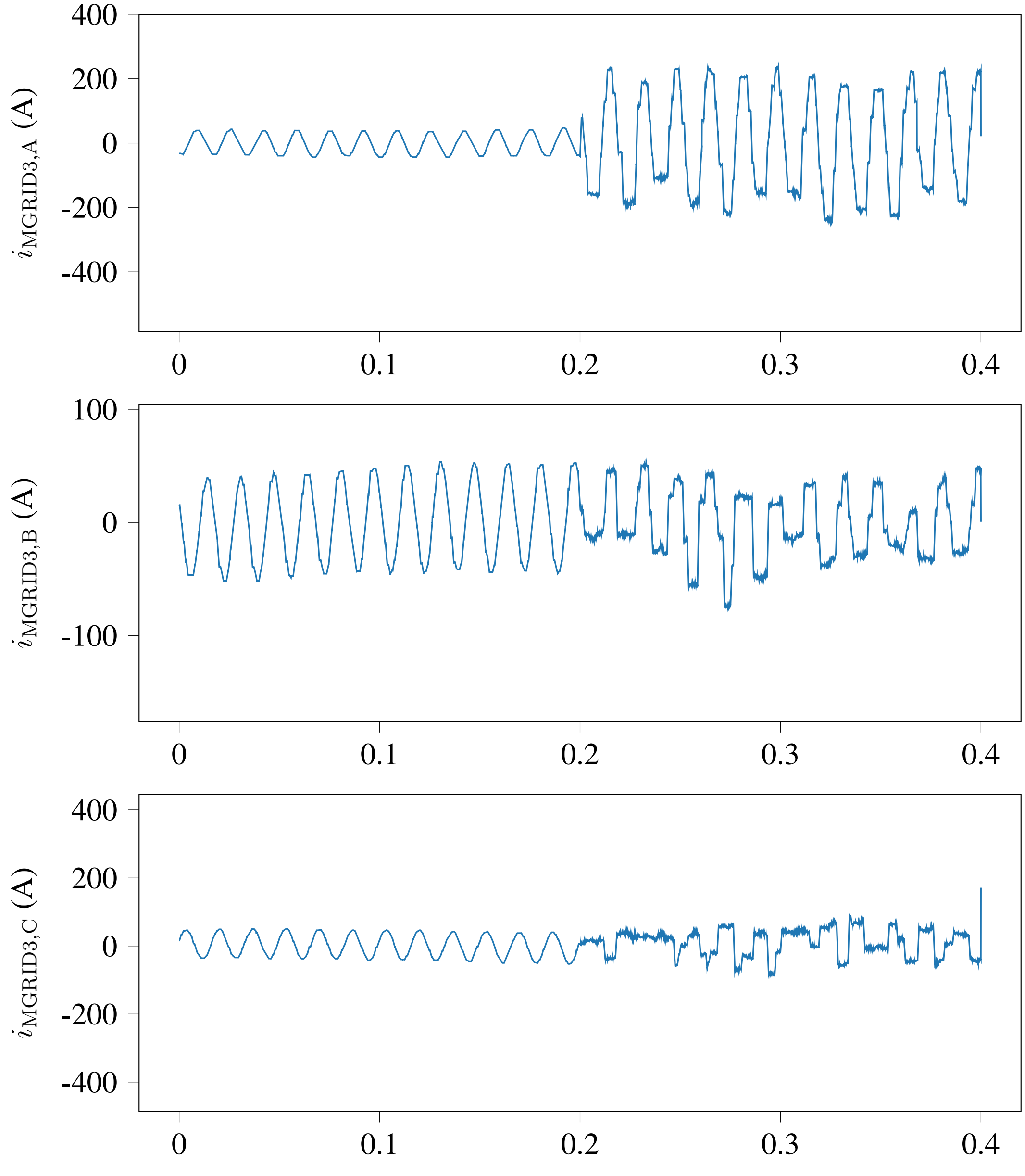

Figure 7.47: Current waveforms recorded by the MU3A IED.

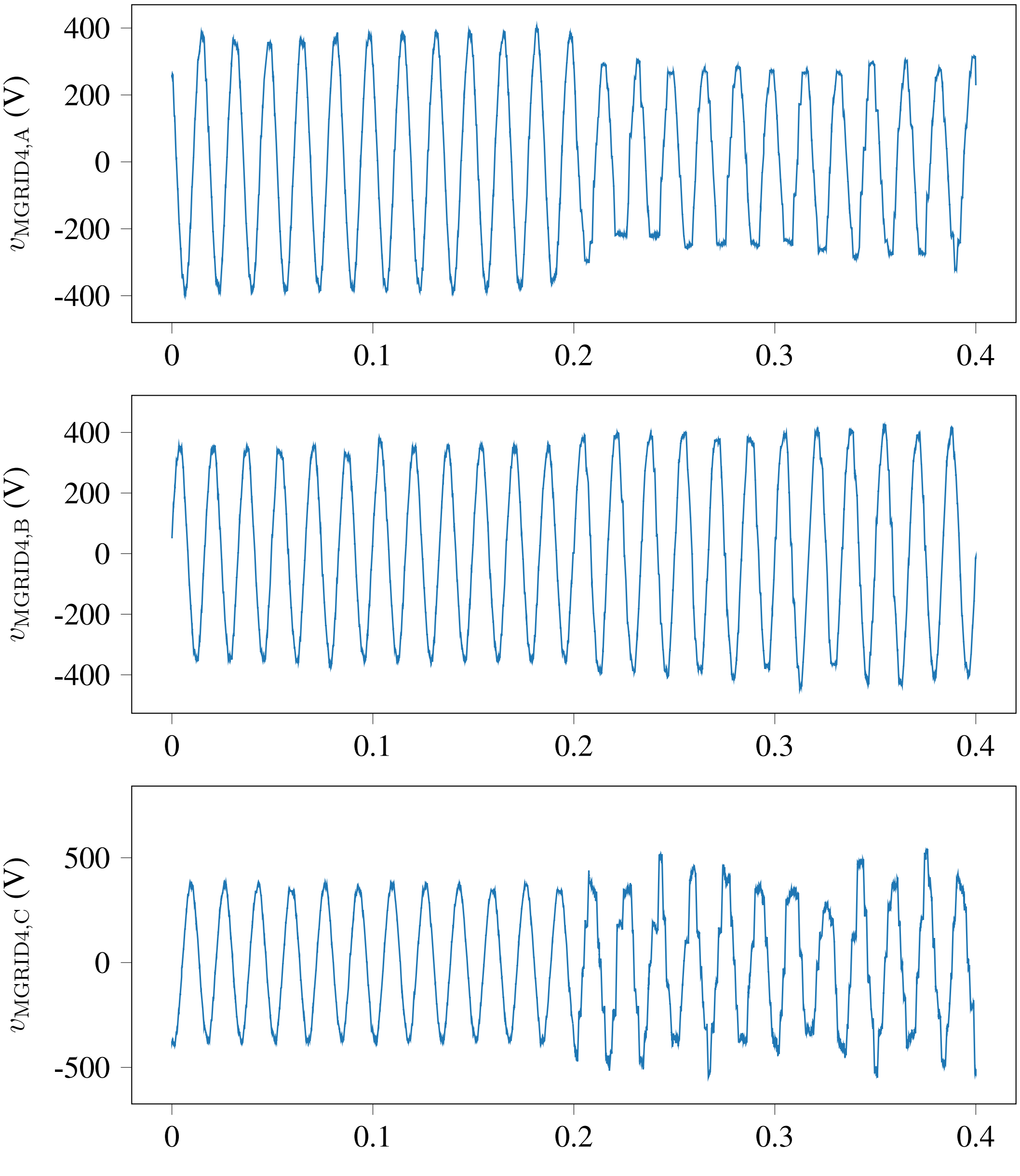

Figure 7.48: Voltage waveforms recorded by the MU4B IED.

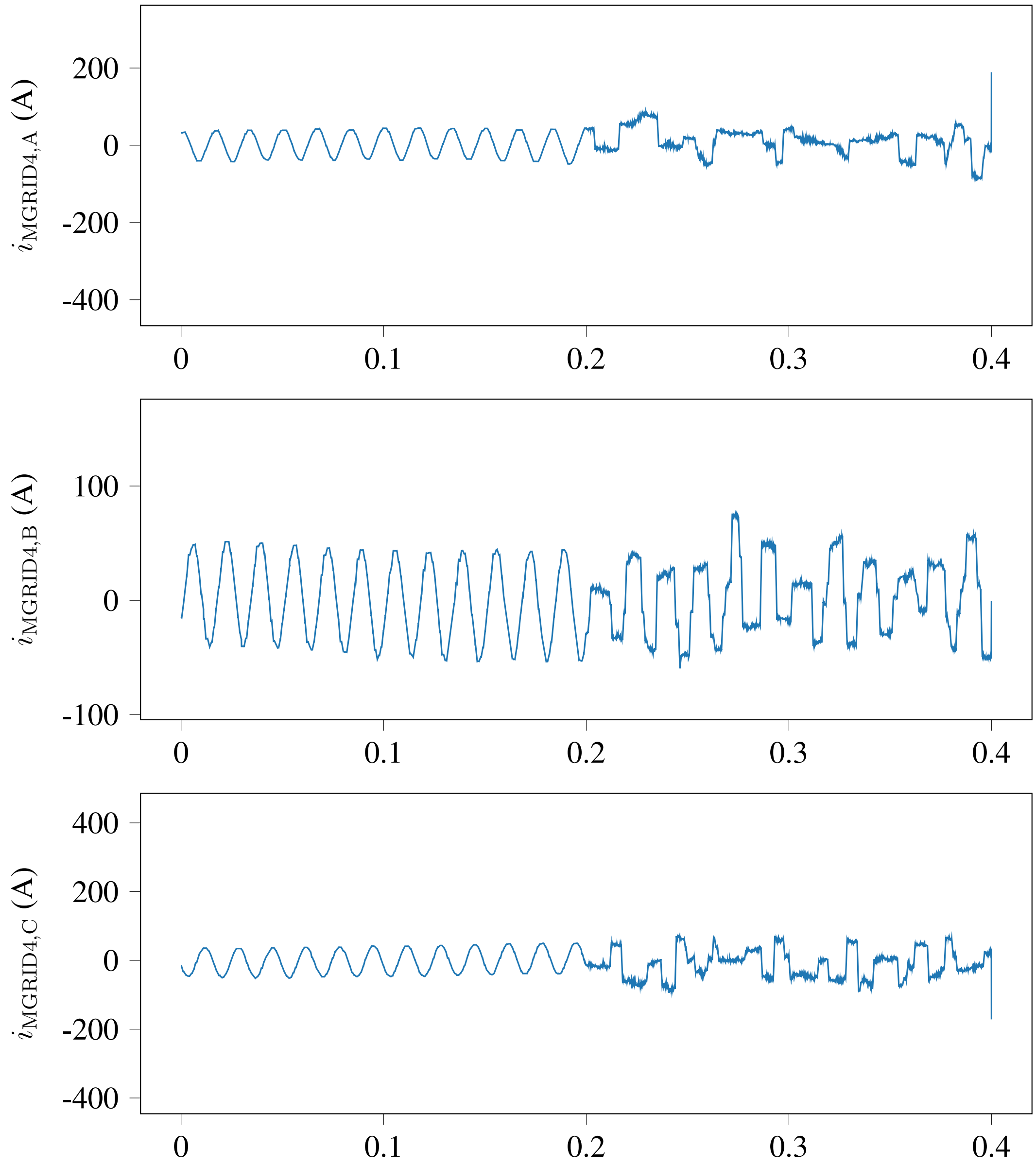

Figure 7.49: Current waveforms recorded by the MU4B IED.

All microgrid protection zones are again under the continuous monitoring of protective relays. A settingless relay monitoring the affected protection zone is designed to trip the zone breakers after noticing that the zone measurements do not fit the model of a healthy cable anymore following the fault initiation at 200 ms. Legacy protection schemes are also expected to detect this type of fault. Regardless of its type, the individual protection zone relay that detects the fault is responsible for the disconnection of the cable between buses MGRID3 and MGRID4 to protect people and equipment. Since this is a case of a legitimate fault happening within the system, the centralized protection scheme proposed in this thesis should allow the disconnection of the cable. The following paragraphs demonstrate how exactly this happens.

Unlike what happens with various individual zone relays, the centralized protection scheme has access to measurements both from within the zone (from MU3A and MU4B) and from outside of the zone (from MU3B, MU4A and MU4C). For comparison purposes, the calculated phasors for phase A quantities are provided in Figures 7.50 and 7.51 for all measurement streams in Table 7.8. It is worth observing that primary and secondary measurements are essentially identical here, as all IEDs record the actual situation within the protection zone. The novel protection scheme utilizes DSE to detect the fault.

Protection algorithm execution

The novel centralized protection scheme begins the by now familiar process of automatically forming a microgrid measurement model based on the individual object-oriented device models, knowledge of the system topology, and the algorithms presented in this document.

Figure 7.52 shows the calculated confidence level, as well as the magnitude and angle measurements for the $i_{\mathrm{MGRID3,A}}$ phasor, and the corresponding absolute normalized residuals for the real and imaginary parts of the phasor. As was the case with the FDIA scenario, the absolute normalized residuals correspond to rectangular quantities, since the internal

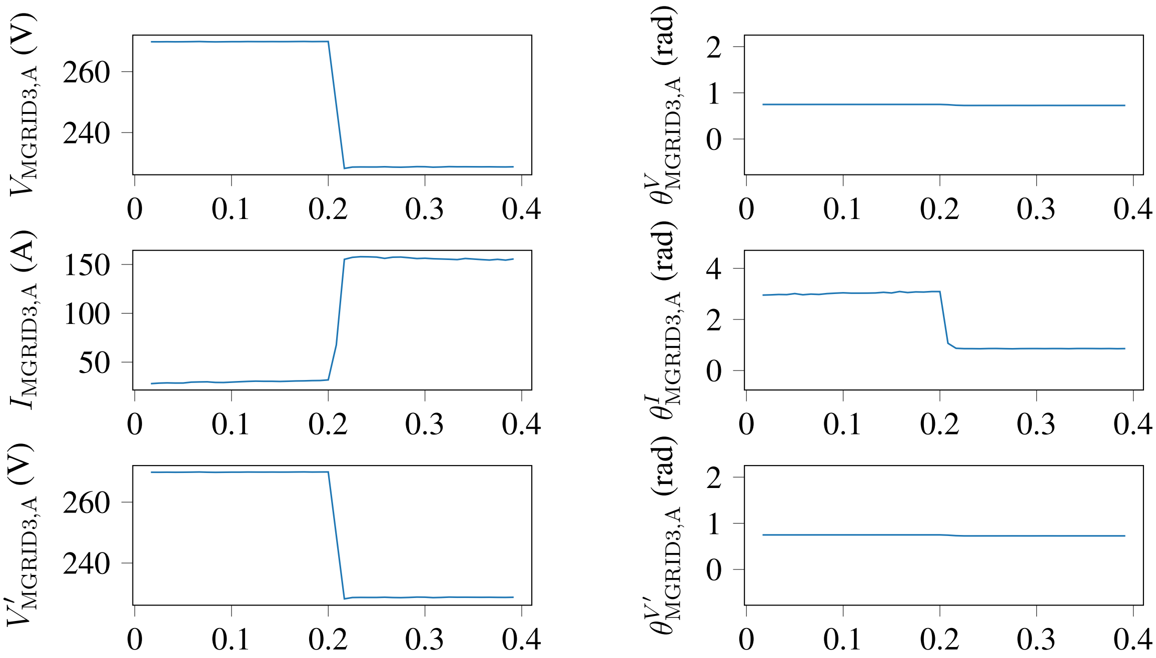

Figure 7.50: Calculated phasors for the MU3A IED.

calculations for the introduced scheme are performed using rectangular coordinates. Moreover, the hypothesis testing module is deactivated in Figure 7.52 for comparison purposes.

The protection scheme executes DSE at each time step using the recorded phasor measurement streams, and calculates the corresponding confidence level. Before the initiation of the fault, the calculated confidence level values are large as expected with the minimum being equal to 99.97%. This is the same value found in the case of the cyber-attack on the detailed microgrid, which is expected since the behavior of the microgrid up to this point should be similar in both cases. This time though, the confidence level collapse is more gradual.

The first DSE execution after the fault finds that the phasors have minimal changes, so it yields a high confidence level equal to 93.77%. The protection scheme is triggered on the next step, as the confidence level then is only 14.31%, which is lower than the selected threshold.

If the protection scheme is allowed to continue calculating confidence levels beyond

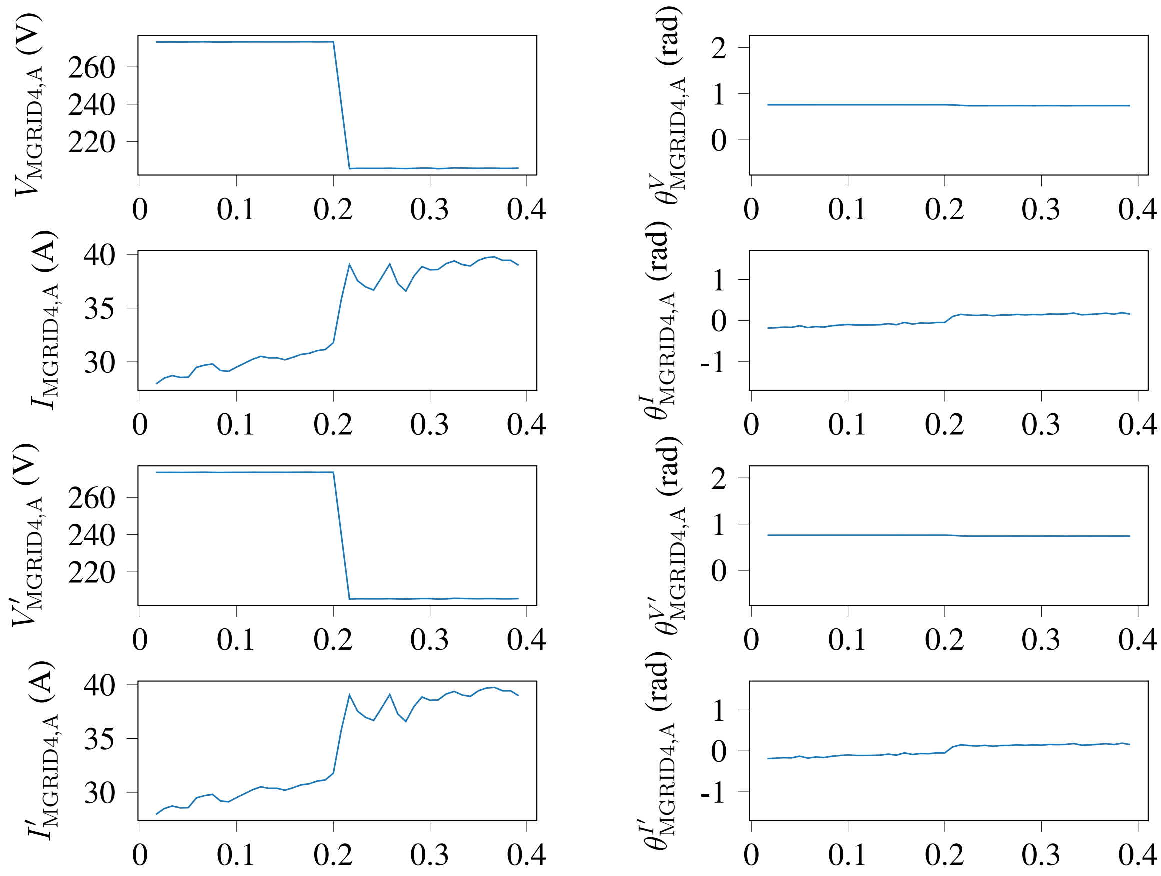

Figure 7.51: Calculated phasors for the MU4B IED.

this point, the confidence level values calculated on the next two steps are 4.66% and less than 6.60% respectively, which shows once more that the reaction of the scheme is quite rapid. Such a collapse of the confidence level between roughly 100% and less than 10% happens within three steps here, which implies a reaction time of at most two cycles. Again, this is a major advantage of the proposed approach.

It should be noted that in this case the confidence level remains around 5% after its collapse, and it does not fall below 1%, as was the case with the cyber-attack scenario. This can be seen in Figure 7.52. This confidence level is still very low and clearly below any reasonable threshold c_t, so the introduced centralized protection scheme still exhibits a desirable outcome.

Going back to the step where the confidence level fell to 14.31%, the absolute normal-

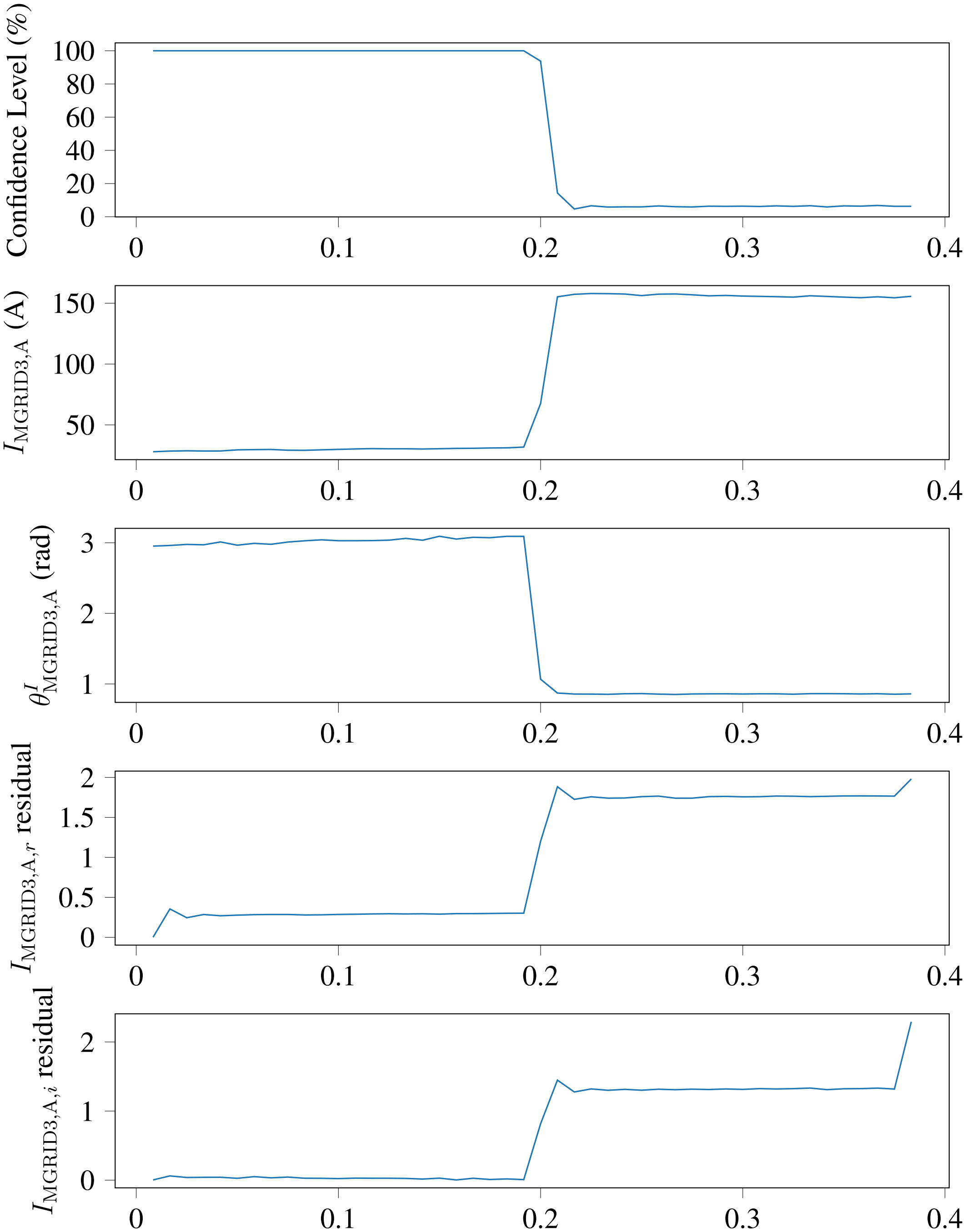

Figure 7.52: Microgrid confidence level, $i_{\mathrm{MGRID3,A}}$ measurements, and corresponding absolute normalized residuals (without hypothesis testing).

ized residuals r_n of Table 7.10 are extracted. This table contains the ten largest absolute normalized residuals from within the affected protection zone, and also shows the corresponding measurements and instrumentation channels. This is crucial information for the execution of the hypothesis testing module.

Table 7.10: Second Microgrid Test System: Suspect measurements under power fault

r_n	Measurement	Instrumentation Channel
1.884	$i_{\mathrm{MGRID3,A}}$	MU3A
1.448	$i_{\mathrm{MGRID3,A}}$	MU3A
0.963	$v'_{\mathrm{MGRID3,C}}$	MU3B
0.892	$i_{\mathrm{MGRID4,A}}$	MU4B
0.892	$i'_{\mathrm{MGRID4,A}}$	MU4A & MU4C
0.729	$v'_{\mathrm{MGRID3,B}}$	MU3B
0.646	$i_{\mathrm{MGRID4,A}}$	MU4B
0.646	$i'_{\mathrm{MGRID4,A}}$	MU4A & MU4C
0.415	$i_{\mathrm{MGRID3,C}}$	MU3A
0.358	$v_{\mathrm{MGRID3,B}}$	MU3A

The reader may again observe that three measurements, namely $i_{\mathrm{MGRID3,A}}$, $i_{\mathrm{MGRID4,A}}$ and $i'_{\mathrm{MGRID4,A}}$ appear in the table twice. This is expected, since the internal computations of the novel centralized protection scheme are performed with complex numbers in rectangular form, so each time domain waveform corresponds to a real and an imaginary residual.

The first suspect measurement is $i_{\mathrm{MGRID3,A}}$, which comes from the MU3A IED. Therefore, all six measurements from this measuring device are grouped together and eliminated. These measurements are $v_{\mathrm{MGRID3,A}}$, $v_{\mathrm{MGRID3,B}}$, $v_{\mathrm{MGRID3,C}}$, $i_{\mathrm{MGRID3,A}}$, $i_{\mathrm{MGRID3,B}}$, and $i_{\mathrm{MGRID3,C}}$. Afterwards, the microgrid measurement model is updated, and the DSE calculation step is repeated using the reduced model this time. This action is not sufficient to restore the confidence level to an acceptable value though. Therefore, the second hypothesis is tested, namely the scenario that a fault has happened within the protection zone. This time, all measurements corresponding to the suspect protection zone, i.e., all measurements from Table 7.8, are eliminated from the microgrid measurement model. This means that the microgrid measurement model contains no trace of the affected zone this time. That is sufficient to restore the microgrid confidence level, thus demonstrating that a discrepancy between the model of at least one microgrid protection zone and all of its corresponding measurements actually exists. The existence of such a discrepancy shows that a power fault is indeed happening.

Figure 7.53 shows the same quantities as Figure 7.52, but this time with the hypothesis testing and measurement elimination module activated.

The observations that can be made here are the following. First, the measurement elimination restored the confidence level to a normal value, thus affirming the root cause of the drop. There is only one step with visibly low confidence level in Figure 7.53, and that confidence level is equal to 14.31%. Since the chosen threshold is 60%, the hypothesis testing is triggered. Once again, the activation of the hypothesis testing module means that the removed measurements are not used anymore, so their normalized residuals are equal to zero for the rest of the interval, as is evident in Figure 7.53.

Hence, any relay responsible the affected zone is allowed to trip the zone breakers, thus disconnecting the cable between MGRID3 and MGRID4. The operation of the novel centralized protection scheme is once again proven to be quick, which is crucial for the safety of both people and power system equipment.

Figures 7.54 and 7.55 show the microgrid confidence level again, as well as the calculated phasor magnitude and angle, and calculated absolute normalized residuals in rectangular form for the $v'_{\mathrm{MGRID3,C}}$ measurement, i.e., the measurement with the third highest normalized residual in Table 7.10. Once more, the changes in this waveform after the initiation of the attack coincide with the confidence level drop and the rise in the value of the absolute normalized residuals corresponding to this measurement. The removal of this measurement can also be verified, since the relevant absolute normalized residuals remain at zero for the rest of the time window after the hypothesis testing module activation.

The next highest absolute normalized residual belongs to the $i_{\mathrm{MGRID4,A}}$ waveform. Figures 7.56 and 7.57 show the microgrid confidence level again, as well as the calculated phasor magnitude and angle, and calculated absolute normalized residuals in rectangular

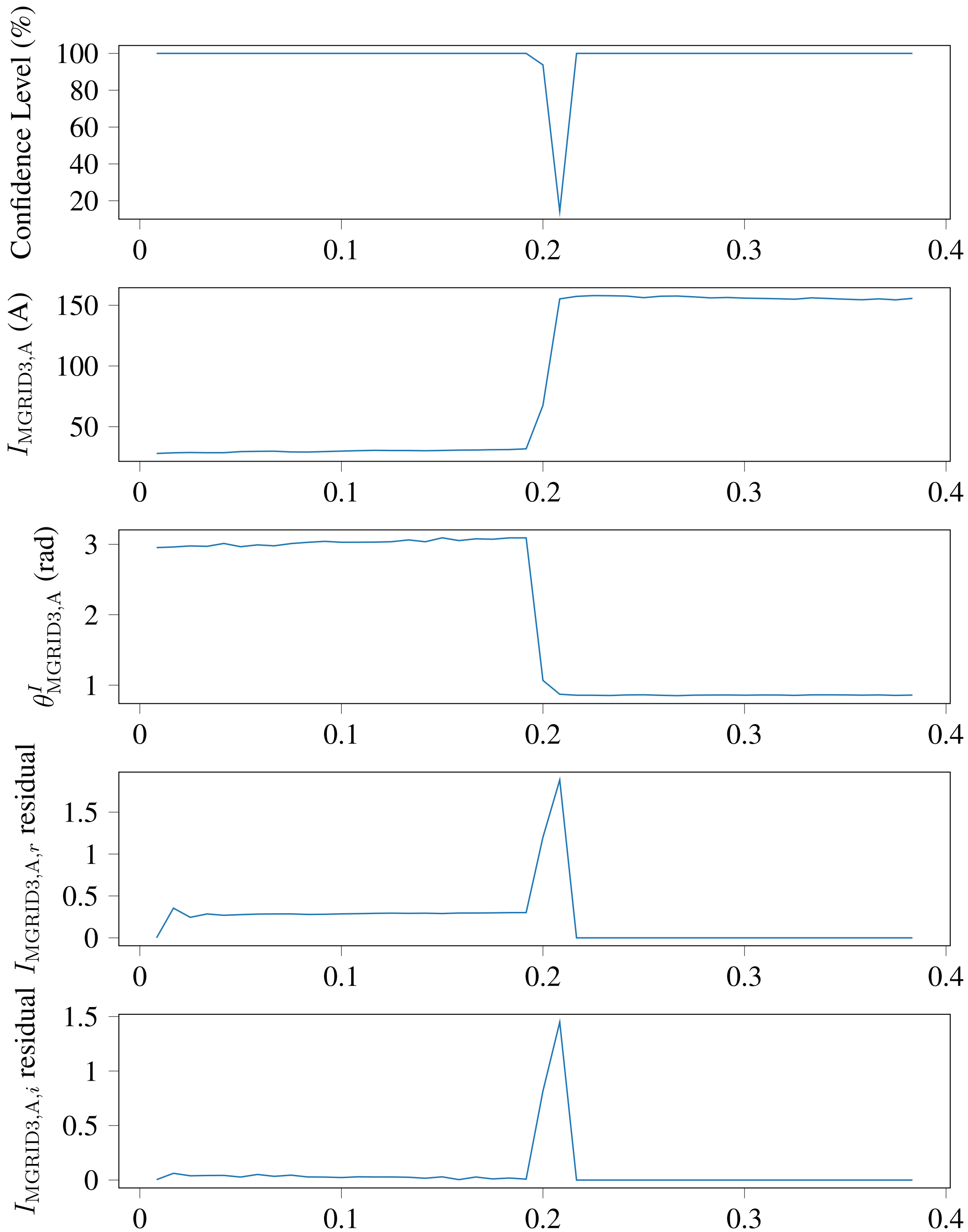

Figure 7.53: Microgrid confidence level, $i_{\mathrm{MGRID3,A}}$ measurements, and corresponding absolute normalized residuals (with hypothesis testing).

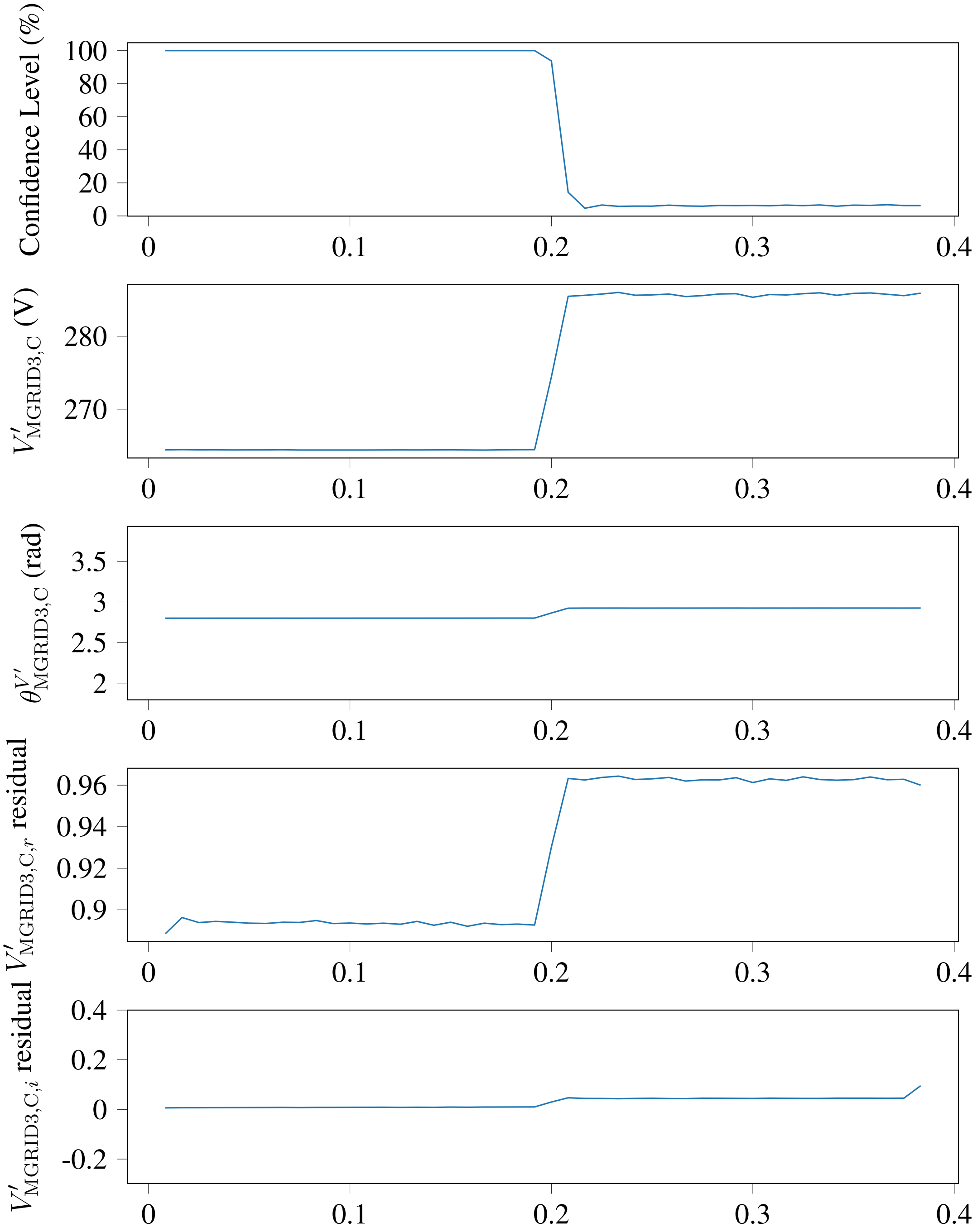

Figure 7.54: Microgrid confidence level, $v'_{\mathrm{MGRID3,C}}$ measurements, and corresponding absolute normalized residuals (without hypothesis testing).

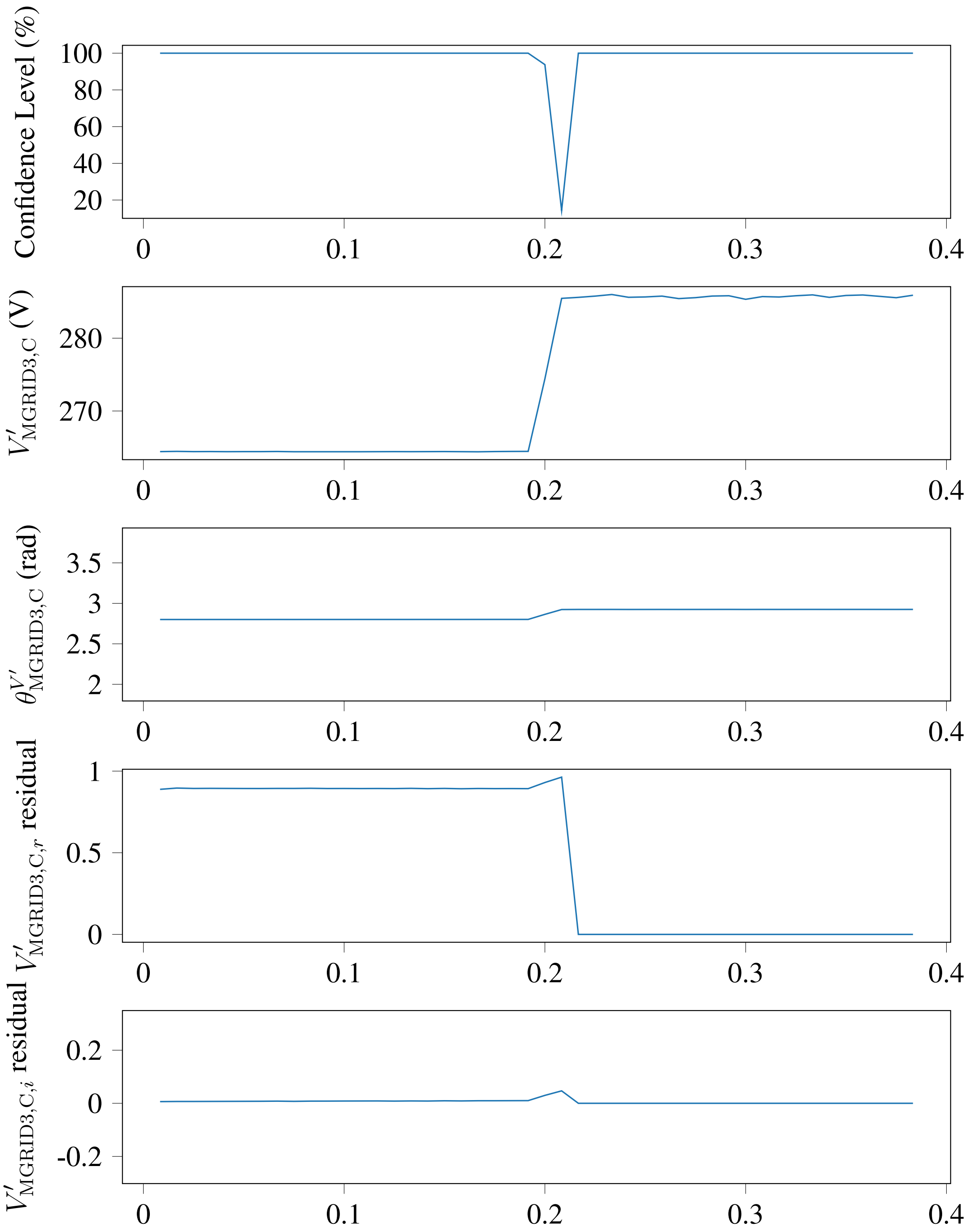

Figure 7.55: Microgrid confidence level, $v'_{\mathrm{MGRID3,C}}$ measurements, and corresponding absolute normalized residuals (with hypothesis testing).

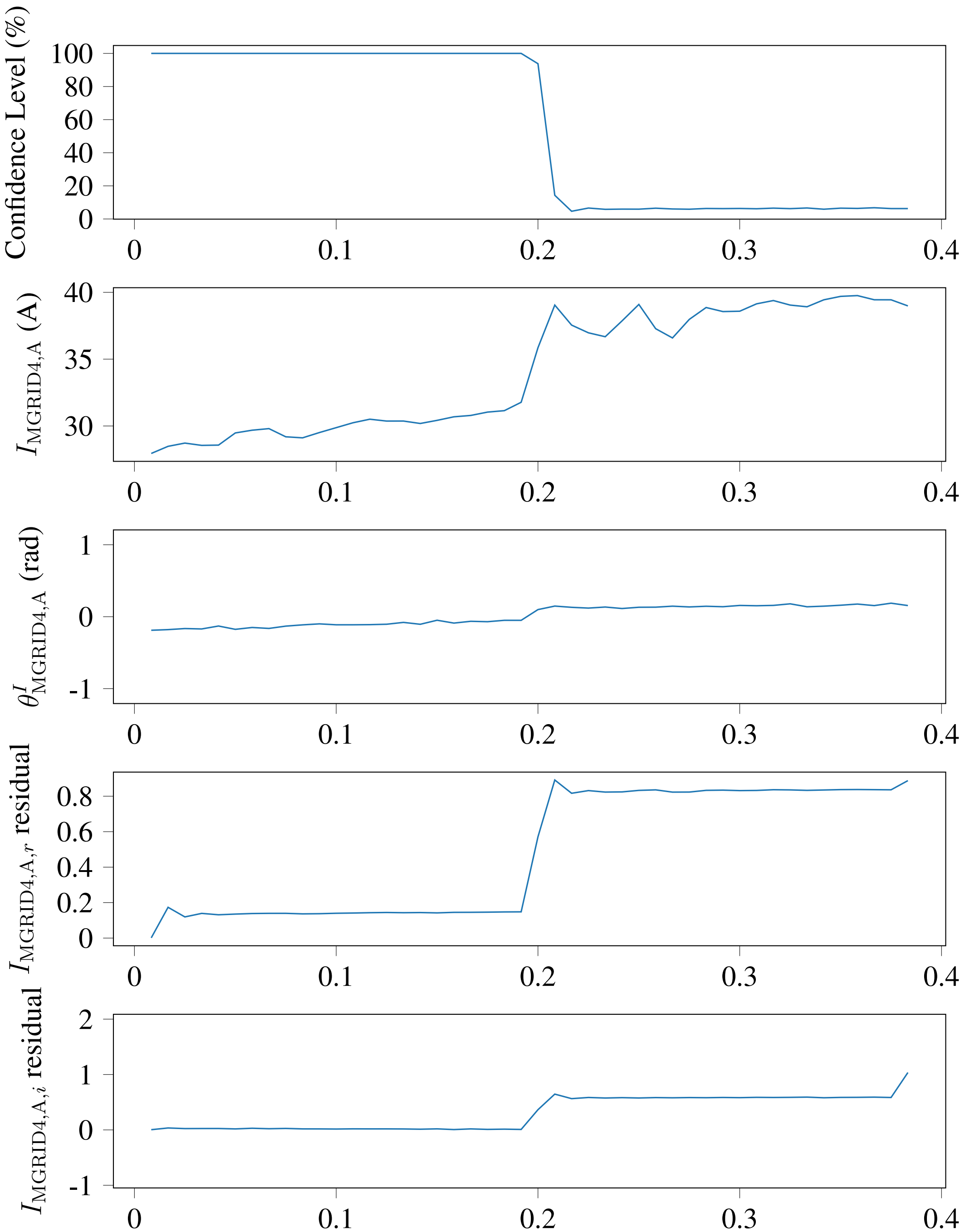

Figure 7.56: Microgrid confidence level, $i_{\mathrm{MGRID4,A}}$ measurements, and corresponding absolute normalized residuals (without hypothesis testing).

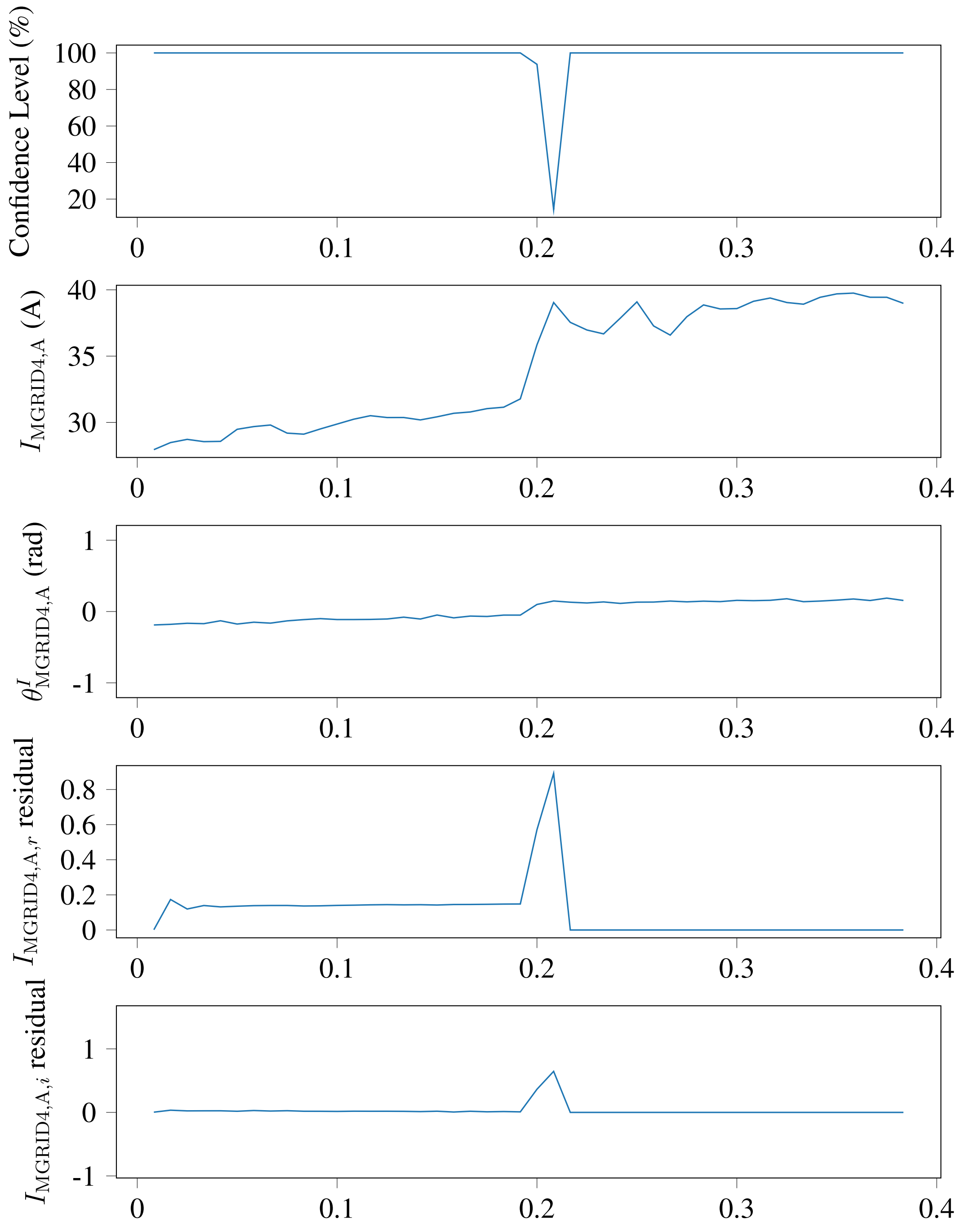

Figure 7.57: Microgrid confidence level, $i_{\text{MGRID4,A}}$ measurements, and corresponding absolute normalized residuals (with hypothesis testing).

form for this measurement. The $i_{\mathrm{MGRID4,A}}$ waveform is part of the affected protection zone, so it must be removed alongside every other zone measurement. This is indeed what happens, as Figure 7.57 shows that the corresponding absolute normalized residuals go to zero after the activation of the hypothesis testing module.

7.3 Summary

This section demonstrated the proper operation of the proposed centralized protection scheme in the presence of both cyber-attacks and power faults. The scheme was tested on two different microgrids, each time for both a cyber-attack scenario and a fault scenario. The scheme was able to successfully distinguish between the two scenarios and issue appropriate commands in each case. Moreover, the introduced protection scheme operated correctly even in the presence of harmonics, which is a necessary quality for such a scheme due to the penetration of inverter-interfaced DERs in microgrids.

CHAPTER 8
CONCLUSION

The final chapter of this dissertation offers some concluding remarks and also highlights the main contributions of the presented research work, as well as suggestions for possible paths for future research.

8.1 Remarks

The presented simulations show that the proposed scheme can correctly distinguish between a fault within a protection zone and a cyber-attack targeting a measurement channel of a microgrid.

It operates quickly in both cases, as it essentially only needs enough samples for the calculated phasor(s) of quantities with abnormal behavior to significantly change. This makes the reaction time dependent on the size of the time window selected for phasor calculation. Here, a window of one cycle is used, so all phasors have fully changed roughly 17 ms after the initiation of any incident, and are usually sufficiently changed for the scheme to operate even earlier. Speed is crucial for the introduced centralized protection scheme, because the source of the discrepancy between the protection zone model and measurements must be identified before the individual zone relays can trip the corresponding zone breakers.

Moreover, it is worth commenting on the choice of absolute normalized residuals as suspect measurement indicators. As normalized residuals are a byproduct of the DSE step, the computational overhead to detect potentially suspect measurements is minimal. Furthermore, while there are no theoretical guarantees, in practice the novel protection algorithm is needed only once to enter the hypothesis testing procedure when isolating the cause of the abnormality in every different scenario used for testing. In the examples presented in this thesis, this observation holds true in the presence of both tampered measurements and power faults. Specifically, in the case of tampered measurements the absolute normalized residuals of the affected measurements are much larger than the rest, thus helping identify the measurement spoofing attack immediately. Likewise, in the case of power faults, all normalized residuals of each affected zone have clearly larger magnitudes than the normalized residuals of all the other protection zones, which makes fault detection fast. Thus, choosing this metric as an indicator of suspect measurements also facilitates the speedy reaction of the protection scheme.

Upon operating, the novel protection scheme eliminates the distorted waveforms and restores the confidence level to its normal value. Therefore, the microgrid is protected against both power faults and cyber intrusions.

8.2 Contributions

The main contributions of this thesis are the following:

- Adaptation of a proven concept used in the area of power system protection to the area of microgrid cybersecurity.

- Definition of an object-oriented syntax capable of describing any microgrid device model in both the time and the quasi-dynamic domains.

- Creation of a system that classifies all microgrid measurements based on their corresponding protection zone and recording device.

- Development of a module that converts time domain measurements to phasors, if necessary.

- Creation of an automated process to build a high-fidelity microgrid measurement model based on knowledge of individual device models and microgrid topology.

- Development of a flexible object-oriented DSE module that calculates the goodness of fit of recorded measurements to the microgrid measurement model.

- Utilization of confidence level as a goodness of fit metric to detect abnormalities.
- Development of a method that performs hypothesis testing to automatically identify suspect measurements, if an abnormality is detected, and uses the measurement classification system and the flexible DSE module to discover the root cause of the abnormality.

8.3 Recommendations for future research

The research work presented in this thesis offers promising possibilities for expansion.

Since the proposed protection approach relies heavily on detailed microgrid device models, there is always a need for a wide variety of models describing different components that might be found in a microgrid. For example, for the purposes of this thesis different single-phase and three-phase transformer models were used, and there will always be more transformers available to install in a microgrid that do not already have SCAQCF descriptions.

Moreover, while this thesis focused on microgrid protection, it is worth considering the application of these ideas on systems larger than a microgrid such as a distribution feeder. This can happen in conjunction with a Distribution Management System (DMS). An example of a DMS that can be expanded to include the ideas of this thesis is presented in [69]. If such an effort is undertaken, the main challenge is expected to be the accommodation of delays caused by the fact that communication lines will be longer, thus increasing communication delays. The number of devices in a substation feeder is also expected to be substantially larger.

While the protection scheme proposed in this thesis works in the quasi-dynamic domain, such a scheme could possibly work at the time domain too. The main challenges in this case are the following. First and foremost, the increase in computational burden will be very significant. For example, assuming a sampling rate of 4.8 kHz, and a full execution of the estimator at every sampling step, that would increase the amount of DSE execution steps by a factor of 40. Moreover, a time domain adaptation of the proposed protection scheme may be more sensitive to communication issues such as dropped measurements, as the time domain samples will not be aggregated into phasors anymore.

Finally, since the novel protection scheme of this thesis is designed in an object-oriented way with interoperability in mind, it is worth considering its inclusion as a module to a microgrid management system, such as the modular microgrid management system presented in [70]. Thus, a management system that can serve as a form of operating system for a wide variety of microgrids can be achieved.

Appendices

APPENDIX A
TRANSFORMER MODELING

This appendix presents a model for a three-phase transformer with inter-turn fault simulation capability and a nonlinear magnetic core [71]. Three single-phase transformers appropriately connected are used as building blocks of the three-phase transformer. The proposed model was utilized to obtain the numerical results presented in section 7.1, as well as in [27]. The modeling steps shown next offer a good demonstration of the process to describe any microgrid device in SCAQCF.

A.1 Compact Device Model

The single-phase model schematic is presented in Figure A.1.

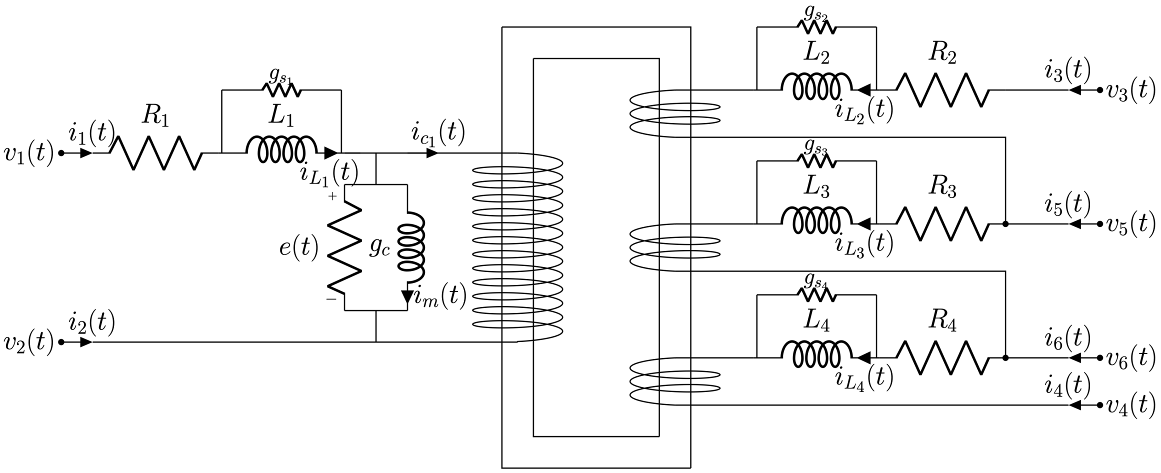

Figure A.1: Single-phase transformer schematic.

The single-phase model equations are the following:

$$i_1(t) = i_{L_1}(t) + g_{s_1} L_1 \frac{di_{L_1}(t)}{dt}, \tag{A.1}$$

$$i_2(t) = -i_{L_1}(t) - g_{s_1} L_1 \frac{di_{L_1}(t)}{dt}, \tag{A.2}$$

$$i_3(t) = i_{L_2}(t) + g_{s_2} L_2 \frac{di_{L_2}(t)}{dt}, \tag{A.3}$$

$$i_4(t) = -i_{L_4}(t) - g_{s_4} L_4 \frac{di_{L_4}(t)}{dt}, \tag{A.4}$$

$$\begin{aligned} i_5(t) = -i_{L_2}(t) - g_{s_2} L_2 \frac{di_{L_2}(t)}{dt} + i_{L_3}(t) \\ + g_{s_3} L_3 \frac{di_{L_3}(t)}{dt}, \end{aligned} \tag{A.5}$$

$$\begin{aligned} i_6(t) = -i_{L_3}(t) - g_{s_3} L_3 \frac{di_{L_3}(t)}{dt} + i_{L_4}(t) \\ + g_{s_4} L_4 \frac{di_{L_4}(t)}{dt}, \end{aligned} \tag{A.6}$$

$$\begin{aligned} 0 = v_1(t) - v_2(t) - R_1 \left(i_{L_1}(t) + g_{s_1} L_1 \frac{di_{L_1}(t)}{dt} \right) \\ - L_1 \frac{di_{L_1}(t)}{dt} - e(t), \end{aligned} \tag{A.7}$$

$$\begin{aligned} 0 = v_3(t) - v_5(t) - R_2 \left(i_{L_2}(t) + g_{s_2} L_2 \frac{di_{L_2}(t)}{dt} \right) \\ - L_2 \frac{di_{L_2}(t)}{dt} - \frac{N_2}{N_1}(1-\alpha) e(t), \end{aligned} \tag{A.8}$$

$$\begin{aligned} 0 = v_5(t) - v_6(t) - R_3 \left(i_{L_3}(t) + g_{s_3} L_3 \frac{di_{L_3}(t)}{dt} \right) \\ - L_3 \frac{di_{L_3}(t)}{dt} - \frac{N_2}{N_1}(\alpha-\beta) e(t), \end{aligned} \tag{A.9}$$

$$\begin{aligned} 0 = v_6(t) - v_4(t) - R_4 \left(i_{L_4}(t) + g_{s_4} L_4 \frac{di_{L_4}(t)}{dt} \right) \\ - L_4 \frac{di_{L_4}(t)}{dt} - \frac{N_2}{N_1}\beta e(t), \end{aligned} \tag{A.10}$$

$$\begin{aligned} 0 = i_{L_1}(t) + g_{s_1} L_1 \frac{di_{L_1}(t)}{dt} - i_{c_1}(t) - i_m(t) \\ - g_c e(t), \end{aligned} \tag{A.11}$$

$$\begin{aligned} 0 = i_{c_1}(t) + \frac{N_2}{N_1}((1-\alpha) i_3(t) + (\alpha-\beta)(i_3(t) + i_5(t)) \\ + \beta(i_3(t) + i_5(t) + i_6(t))), \end{aligned} \tag{A.12}$$

$$0 = e(t) - \frac{d\lambda(t)}{dt}, \tag{A.13}$$

$$0 = i_m(t) - i_0 \left| \frac{\lambda(t)}{\lambda_0} \right|^n \text{sign}(\lambda(t)), \tag{A.14}$$

where $v_1(t)$, $v_2(t)$, $v_3(t)$, $v_4(t)$, $v_5(t)$, $v_6(t)$, $i_{L_1}(t)$, $i_{L_2}(t)$, $i_{L_3}(t)$, $i_{L_4}(t)$, $i_{c_1}(t)$, $e(t)$, $\lambda(t)$, $i_m(t)$ are the device model states. The device model parameters include α, which is a parameter that denotes the percentage of secondary winding turns between node 4 and node 5, and β which is a parameter that denotes the percentage of secondary winding turns between node 4 and node 6. Furthermore, g_c, i_0 and λ_0 are transformer core parameters, N_1 and N_2 are the number of turns in the primary and secondary winding of the transformer respectively, R_1, R_2, R_3, R_4 are the transformer winding resistances, and L_1, L_2, L_3, L_4 are the transformer winding leakage inductances.

In addition, the conductances g_{s_1}, g_{s_2}, g_{s_3} and g_{s_4} are introduced to eliminate possible numerical problems [72]. The errors introduced by this step are orders of magnitude smaller than the measurement errors, so this choice does not have an adverse effect on the presented simulations. Finally, the assumption that the resistance and inductance of the secondary winding are distributed in three different segments improves the accuracy of the transformer model.

A.2 State and Control Algebraic Quadratized Device Model

A device described in SCQDM form in the quasi-dynamic domain uses the equations in Section 4.3. The corresponding time domain SCQDM equations are very similar, and they are introduced here. These are

$$\mathbf{i}(t) = Y_{\text{eqx1}}\mathbf{x}(t) + Y_{\text{equ1}}\mathbf{u}(t) + D_{\text{eqxd1}}\frac{d\mathbf{x}}{dt}(t) + \mathbf{C}_{\text{eqc1}}, \tag{A.15}$$

$$\mathbf{0} = Y_{\text{eqx2}}\mathbf{x}(t) + Y_{\text{equ2}}\mathbf{u}(t) + D_{\text{eqxd2}}\frac{d\mathbf{x}}{dt}(t) + \mathbf{C}_{\text{eqc2}}, \tag{A.16}$$

$$\mathbf{0} = Y_{\mathrm{eqx3}}\mathbf{x}(t) + Y_{\mathrm{equ3}}\mathbf{u}(t) + \left\{\begin{matrix} \vdots \\ \mathbf{x}(t)^{\top} F^{i}_{\mathrm{eqxx3}} \mathbf{x}(t) \\ \vdots \end{matrix}\right\}$$

$$+ \left\{\begin{matrix} \vdots \\ \mathbf{u}(t)^{\top} F^{i}_{\mathrm{equu3}} \mathbf{u}(t) \\ \vdots \end{matrix}\right\} + \left\{\begin{matrix} \vdots \\ \mathbf{u}(t)^{\top} F^{i}_{\mathrm{equx3}} \mathbf{x}(t) \\ \vdots \end{matrix}\right\} + \mathbf{C}_{\mathrm{eqc3}}, \tag{A.17}$$

$$\mathbf{g}\left(\mathbf{x}, \mathbf{u}\right) = Y_{\mathrm{hfeqx}}\mathbf{x}(t) + Y_{\mathrm{hfequ}}\mathbf{u}(t) + \left\{\begin{matrix} \vdots \\ \mathbf{x}(t)^{\top} F^{i}_{\mathrm{hfeqxx}} \mathbf{x}(t) \\ \vdots \end{matrix}\right\}$$

$$+ \left\{\begin{matrix} \vdots \\ \mathbf{u}(t)^{\top} F^{i}_{\mathrm{hfequu}} \mathbf{u}(t) \\ \vdots \end{matrix}\right\} + \left\{\begin{matrix} \vdots \\ \mathbf{u}(t)^{\top} F^{i}_{\mathrm{hfequx}} \mathbf{x}(t) \\ \vdots \end{matrix}\right\} + \mathbf{C}_{\mathrm{hfeqc}}, \tag{A.18}$$

$$\text{subject to} \quad \mathbf{g}\left(\mathbf{x}, \mathbf{u}\right) \leq \mathbf{0}, \tag{A.19}$$

$$\mathbf{u}_{\mathrm{hmin}} \leq \mathbf{u}(t) \leq \mathbf{u}_{\mathrm{hmax}}, \tag{A.20}$$

$$\mathbf{x}_{\mathrm{hmin}} \leq \mathbf{x}(t) \leq \mathbf{x}_{\mathrm{hmax}}. \tag{A.21}$$

Here, $\mathbf{i}$ denotes the terminal through variable vector, $\mathbf{x}$ is the state variable vector, $\mathbf{u}$ represents the control variable vector, $\mathbf{x}_{\mathrm{hmin}}$, $\mathbf{x}_{\mathrm{hmax}}$, $\mathbf{u}_{\mathrm{hmin}}$, $\mathbf{u}_{\mathrm{hmax}}$ are appropriate limits on state and control variables, $\mathbf{g}$ is the constraint vector function, Y_{eqx1}, Y_{eqx2}, Y_{eqx3}, Y_{hfeqx} are coefficient matrices for state variables, Y_{equ1}, Y_{equ2}, Y_{equ3}, Y_{hfequ} are coefficient matrices for control variables, D_{eqxd1}, D_{eqxd2} are coefficient matrices for first-order derivatives of state variables, F_{eqxx3}, F_{equu3}, F_{equx3}, $F_{\mathrm{hfeqxx}}, F_{\mathrm{hfequu}}, F_{\mathrm{hfequx}}$ are coefficient matrices for quadratic terms, and $\mathbf{C}_{\mathrm{eqc1}}$, $\mathbf{C}_{\mathrm{eqc2}}$, $\mathbf{C}_{\mathrm{eqc3}}$, $\mathbf{C}_{\mathrm{hfeqc}}$ are appropriate constant vectors.

Equations (A.1) to (A.14) need some further manipulation to be able to cast in a form compatible with Equations (A.15) to (A.21).

Specifically, Equations (A.1) to (A.6) become

$$i_1(t) = i_{L_1}(t) + g_{s_1} L_1 \frac{di_{L_1}(t)}{dt}, \tag{A.22}$$

$$i_2(t) = -i_{L_1}(t) - g_{s_1} L_1 \frac{di_{L_1}(t)}{dt}, \tag{A.23}$$

$$i_3(t) = i_{L_2}(t) + g_{s_2} L_2 \frac{di_{L_2}(t)}{dt}, \tag{A.24}$$

$$i_4(t) = -i_{L_4}(t) - g_{s_4} L_4 \frac{di_{L_4}(t)}{dt}, \tag{A.25}$$

$$\begin{aligned} i_5(t) = &-i_{L_2}(t) + i_{L_3}(t) \\ &- g_{s_2} L_2 \frac{di_{L_2}(t)}{dt} + g_{s_3} L_3 \frac{di_{L_3}(t)}{dt}, \end{aligned} \tag{A.26}$$

$$\begin{aligned} i_6(t) = &-i_{L_3}(t) + i_{L_4}(t) \\ &- g_{s_3} L_3 \frac{di_{L_3}(t)}{dt} + g_{s_4} L_4 \frac{di_{L_4}(t)}{dt}, \end{aligned} \tag{A.27}$$

which are the linear through equations of the SCQDM model, thus providing the values to fill matrices Y_{eqx1} and D_{eqxd1}. In this case, matrix Y_{equ1} and vector $\mathbf{C}_{\text{eqc1}}$ contain only zeros.

As far as Equations (A.7) to (A.13) are concerned, they are reformulated as

$$\begin{aligned} 0 = &\, v_1(t) - v_2(t) - R_1 i_{L_1}(t) - e(t) \\ &- L_1 \left(g_{s_1} R_1 + 1\right) \frac{di_{L_1}(t)}{dt}, \end{aligned} \tag{A.28}$$

$$\begin{aligned} 0 = &\, v_3(t) - v_5(t) - R_2 i_{L_2}(t) - \frac{N_2}{N_1}(1-\alpha) e(t) \\ &- L_2 \left(g_{s_2} R_2 + 1\right) \frac{di_{L_2}(t)}{dt}, \end{aligned} \tag{A.29}$$

$$\begin{aligned} 0 = &\, v_5(t) - v_6(t) - R_3 i_{L_3}(t) - \frac{N_2}{N_1}(\alpha-\beta) e(t) \\ &- L_3 \left(g_{s_3} R_3 + 1\right) \frac{di_{L_3}(t)}{dt}, \end{aligned} \tag{A.30}$$

$$
\begin{aligned}
0 &= -v_4(t) + v_6(t) - R_4 i_{L_4}(t) - \frac{N_2}{N_1}\beta e(t) \\
&\quad - L_4\left(g_{s_4} R_4 + 1\right)\frac{di_{L_4}(t)}{dt}, && \text{(A.31)} \\
0 &= i_{L_1}(t) - i_{c_1}(t) - g_c e(t) - i_m(t) \\
&\quad + g_{s_1} L_1 \frac{di_{L_1}(t)}{dt}, && \text{(A.32)} \\
0 &= \frac{N_2}{N_1}(1-\alpha) i_{L_2}(t) + \frac{N_2}{N_1}(\alpha-\beta) i_{L_3}(t) + \frac{N_2}{N_1}\beta i_{L_4}(t) + i_{c_1}(t) \\
&\quad + \frac{N_2}{N_1}(1-\alpha) g_{s_2} L_2 \frac{di_{L_2}(t)}{dt} + \frac{N_2}{N_1}(\alpha-\beta) g_{s_3} L_3 \frac{di_{L_3}(t)}{dt} \\
&\quad + \frac{N_2}{N_1}\beta g_{s_4} L_4 \frac{di_{L_4}(t)}{dt}, && \text{(A.33)} \\
0 &= e(t) - \frac{d\lambda(t)}{dt}, && \text{(A.34)}
\end{aligned}
$$

which are the linear virtual equations of the single-phase transformer SCQDM model. These equations are used to fill matrices Y_{eqx2} and D_{eqxd2}, while matrix Y_{equ2} and vector $\mathbf{C}_{\text{eqc2}}$ contain only zeros.

Finally, the only remaining equation is the magnetizing current equation, i.e.,

$$
0 = i_m(t) - i_0 \left| \frac{\lambda(t)}{\lambda_0} \right|^n \operatorname{sign}(\lambda(t)). \tag{A.35}
$$

Depending on the selected value of the exponent n, this equation can be reformulated as shown in Section 4.2 by adding new SCQDM equations alongside accompanying state variables. These equations provide the quadratic virtual equations of the SCQDM, which means that they are used to fill the Y_{eqx3} and F^i_{eqxx3} matrices. As this model contains neither control variables nor constants, the Y_{equ3}, F^i_{equu3} and F^i_{equx3} matrices, and the $\mathbf{C}_{\text{eqc3}}$ vector contain only zeros.

No other SCQDM equation is needed for this transformer model. Therefore, the final state vector contains the $v_1(t)$, $v_2(t)$, $v_3(t)$, $v_4(t)$, $v_5(t)$, $v_6(t)$, $i_{L_1}(t)$, $i_{L_2}(t)$, $i_{L_3}(t)$, $i_{L_4}(t)$, $i_{c_1}(t)$, $e(t)$, $\lambda(t)$, $i_m(t)$ variables, alongside any new variable introduced during the quadratization of the magnetizing current equation.

Once appropriate numerical values for the parameters in Equations (A.22) to (A.35) are obtained, the SCQDM matrices can finally be filled.

A.3 State and Control Algebraic Quadratic Companion Form

The general form of a device model in quasi-dynamic domain SCAQCF is presented in Section 4.5. Due to the flexibility of this modeling approach, a device model in time domain SCAQCF is described in a very similar way as follows

$$\left\{\begin{matrix} \mathbf{i}(t) \\ \mathbf{0} \\ \mathbf{0} \\ \mathbf{i}(t_m) \\ \mathbf{0} \\ \mathbf{0} \end{matrix}\right\} = Y_{\text{eqx}}\mathbf{x}(t) + Y_{\text{equ}}\mathbf{u}(t) + \left\{\begin{matrix} \vdots \\ \mathbf{x}(t)^\top F^i_{\text{eqxx}}\mathbf{x}(t) \\ \vdots \end{matrix}\right\}$$

$$+ \left\{\begin{matrix} \vdots \\ \mathbf{u}(t)^\top F^i_{\text{equu}}\mathbf{u}(t) \\ \vdots \end{matrix}\right\} + \left\{\begin{matrix} \vdots \\ \mathbf{u}(t)^\top F^i_{\text{equx}}\mathbf{x}(t) \\ \vdots \end{matrix}\right\} - \mathbf{B}_{\text{eq}}, \tag{A.36}$$

$$\mathbf{B}_{\text{eq}} = -N_{\text{eqx}}\mathbf{x}(t-h) - N_{\text{equ}}\mathbf{u}(t-h) - M_{\text{eq}}\mathbf{i}(t-h) - \mathbf{K}_{\text{eq}}, \tag{A.37}$$

$$\mathbf{g}\left(\mathbf{x},\mathbf{u}\right) = Y_{\text{feqx}}\mathbf{x}(t) + Y_{\text{fequ}}\mathbf{u}(t) + \left\{\begin{matrix} \vdots \\ \mathbf{x}(t)^\top F^i_{\text{feqxx}}\mathbf{x}(t) \\ \vdots \end{matrix}\right\}$$

$$+ \left\{\begin{matrix} \vdots \\ \mathbf{u}(t)^\top F^i_{\text{fequu}}\mathbf{u}(t) \\ \vdots \end{matrix}\right\} + \left\{\begin{matrix} \vdots \\ \mathbf{u}(t)^\top F^i_{\text{fequx}}\mathbf{x}(t) \\ \vdots \end{matrix}\right\} + \mathbf{C}_{\text{feqc}}, \tag{A.38}$$

$$\text{subject to}\quad \mathbf{g}\left(\mathbf{x},\mathbf{u}\right) \leq \mathbf{0}, \tag{A.39}$$

$$\mathbf{u}_{\text{min}} \leq \mathbf{u}(t) \leq \mathbf{u}_{\text{max}}, \tag{A.40}$$

$$\mathbf{x}_{\text{min}} \leq \mathbf{x}(t) \leq \mathbf{x}_{\text{max}}. \tag{A.41}$$

For Equations (A.36) to (A.41), $\mathbf{i}$ denotes the terminal through variable vector, $\mathbf{x}$ is the state variable vector, $\mathbf{u}$ represents the control variable vector, $\mathbf{x}_{\text{min}}$, $\mathbf{x}_{\text{max}}$, $\mathbf{u}_{\text{min}}$, $\mathbf{u}_{\text{max}}$ are appropriate limits on state and control variables, $\mathbf{g}$ is the constraint vector function, Y_{eqx}, N_{eqx}, Y_{feqx} are coefficient matrices for state variables, Y_{equ}, N_{equ}, Y_{fequ} are coefficient matrices for control variables, F_{eqxx}, F_{equu}, F_{equx}, F_{feqxx}, F_{fequu}, F_{fequx} are coefficient matrices for quadratic terms, M_{eq} is a coefficient matrix for through variables, and $\mathbf{K}_{\text{eq}}$, $\mathbf{C}_{\text{feqc}}$ are appropriate constant vectors, h is the integration step, and t_m is the midpoint of the integration interval.

Thus, the time domain transformer model presented in this appendix can be cast into SCAQCF through the calculation of the coefficient matrices and vectors in Equations (A.36) to (A.41). These matrices and vectors can be derived from the SCQDM equations using quadratic integration with a time step equal to h. It should be noted that both state and control SCAQCF vectors are double in length compared to their SCQDM counterparts, since quadratically integrating the SCQDM equations introduces states and controls at the integration midpoint t_m to the corresponding vectors. In other words, while the SCQDM vectors for states and controls account only for what happens at time t, their SCAQCF equivalents have components both for time t and for time t_m.

One of the consequences of this, is that the SCQDM limits for state and control, i.e., the $\mathbf{x}_{\text{hmin}}$, $\mathbf{x}_{\text{hmax}}$, $\mathbf{u}_{\text{hmin}}$, $\mathbf{u}_{\text{hmax}}$ vectors are transformed to the following equivalent vectors

$$\mathbf{x}_{\text{min}} = \begin{bmatrix} \mathbf{x}_{\text{hmin}} & \mathbf{x}_{\text{hmin}} \end{bmatrix}^{\mathsf{T}}, \tag{A.42}$$

$$\mathbf{x}_{\max} = \begin{bmatrix} \mathbf{x}_{\text{hmax}} & \mathbf{x}_{\text{hmax}} \end{bmatrix}^{\mathsf{T}}, \tag{A.43}$$

$$\mathbf{u}_{\min} = \begin{bmatrix} \mathbf{u}_{\text{hmin}} & \mathbf{u}_{\text{hmin}} \end{bmatrix}^{\mathsf{T}}, \tag{A.44}$$

$$\mathbf{u}_{\max} = \begin{bmatrix} \mathbf{u}_{\text{hmax}} & \mathbf{u}_{\text{hmax}} \end{bmatrix}^{\mathsf{T}}. \tag{A.45}$$

In this thesis, the conversion from SCQDM to SCAQCF is automatically performed in WinIGS utilizing the following relationships between the SCAQCF coefficient matrices and vectors and the SCQDM coefficient matrices and vectors.

First, the coefficient matrices for state variables are

$$Y_{\text{eqx}} = \begin{bmatrix} \frac{4}{h}D_{\text{eqxd1}} + Y_{\text{eqx1}} & -\frac{8}{h}D_{\text{eqxd1}} \\ \frac{4}{h}D_{\text{eqxd2}} + Y_{\text{eqx2}} & -\frac{8}{h}D_{\text{eqxd2}} \\ Y_{\text{eqx3}} & \mathbf{0} \\ \frac{1}{2h}D_{\text{eqxd1}} & \frac{2}{h}D_{\text{eqxd1}} + Y_{\text{eqx1}} \\ \frac{1}{2h}D_{\text{eqxd2}} & \frac{2}{h}D_{\text{eqxd2}} + Y_{\text{eqx2}} \\ \mathbf{0} & Y_{\text{eqx3}} \end{bmatrix}, \tag{A.46}$$

$$N_{\text{eqx}} = \begin{bmatrix} \frac{4}{h}D_{\text{eqxd1}} - Y_{\text{eqx1}} \\ \frac{4}{h}D_{\text{eqxd2}} - Y_{\text{eqx2}} \\ \mathbf{0} \\ -\frac{5}{2h}D_{\text{eqxd1}} + \frac{1}{2}Y_{\text{eqx1}} \\ -\frac{5}{2h}D_{\text{eqxd2}} + \frac{1}{2}Y_{\text{eqx2}} \\ \mathbf{0} \end{bmatrix}, \tag{A.47}$$

$$Y_{\text{feqx}} = \begin{bmatrix} Y_{\text{hfeqx}} & \mathbf{0} \\ \mathbf{0} & Y_{\text{hfeqx}} \end{bmatrix}. \tag{A.48}$$

Similarly, the coefficient matrices for control variables are

$$Y_{\mathrm{equ}} = \begin{bmatrix} Y_{\mathrm{equ1}} & \mathbf{0} \\ Y_{\mathrm{equ2}} & \mathbf{0} \\ Y_{\mathrm{equ3}} & \mathbf{0} \\ \mathbf{0} & Y_{\mathrm{equ1}} \\ \mathbf{0} & Y_{\mathrm{equ2}} \\ \mathbf{0} & Y_{\mathrm{equ3}} \end{bmatrix}, \tag{A.49}$$

$$N_{\mathrm{equ}} = \begin{bmatrix} -Y_{\mathrm{equ1}} \\ -Y_{\mathrm{equ2}} \\ \mathbf{0} \\ \frac{1}{2}Y_{\mathrm{equ1}} \\ \frac{1}{2}Y_{\mathrm{equ2}} \\ \mathbf{0} \end{bmatrix}, \tag{A.50}$$

$$Y_{\mathrm{fequ}} = \begin{bmatrix} Y_{\mathrm{hfequ}} & \mathbf{0} \\ \mathbf{0} & Y_{\mathrm{hfequ}} \end{bmatrix}. \tag{A.51}$$

Furthermore, the coefficient matrices for quadratic terms are

$$F^i_{\mathrm{eqxx}} = \begin{bmatrix} F^i_{\mathrm{eqxx3}} & \mathbf{0} \\ \mathbf{0} & F^i_{\mathrm{eqxx3}} \end{bmatrix}, \tag{A.52}$$

$$F^i_{\mathrm{equu}} = \begin{bmatrix} F^i_{\mathrm{equu3}} & \mathbf{0} \\ \mathbf{0} & F^i_{\mathrm{equu3}} \end{bmatrix}, \tag{A.53}$$

$$F^i_{\mathrm{equx}} = \begin{bmatrix} F^i_{\mathrm{equx3}} & \mathbf{0} \\ \mathbf{0} & F^i_{\mathrm{equx3}} \end{bmatrix}, \tag{A.54}$$

$$F^i_{\text{feqxx}} = \begin{bmatrix} F^i_{\text{hfeqxx}} & \mathbf{0} \\ \mathbf{0} & F^i_{\text{hfeqxx}} \end{bmatrix}, \tag{A.55}$$

$$F^i_{\text{fequu}} = \begin{bmatrix} F^i_{\text{hfequu}} & \mathbf{0} \\ \mathbf{0} & F^i_{\text{hfequu}} \end{bmatrix}, \tag{A.56}$$

$$F^i_{\text{fequx}} = \begin{bmatrix} F^i_{\text{hfequx}} & \mathbf{0} \\ \mathbf{0} & F^i_{\text{hfequx}} \end{bmatrix}. \tag{A.57}$$

Assuming a device model with a total number of l through variables, and that $\mathbb{I}_n$ denotes an $n \times n$ identity matrix, the coefficient matrix for through variables is

$$M_{\text{eq}} = \begin{bmatrix} \mathbb{I}_l \\ \mathbf{0} \\ \mathbf{0} \\ -\frac{1}{2}\mathbb{I}_l \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix}. \tag{A.58}$$

Finally, the constant vectors are

$$\mathbf{K}_{\text{eq}} = \begin{bmatrix} \mathbf{0} \\ \mathbf{0} \\ \mathbf{C}_{\text{eqc3}} \\ \frac{3}{2}\mathbf{C}_{\text{eqc1}} \\ \frac{3}{2}\mathbf{C}_{\text{eqc2}} \\ \mathbf{C}_{\text{eqc3}} \end{bmatrix}, \tag{A.59}$$

$$\mathbf{C}_{\mathrm{feqc}} = \begin{bmatrix} \mathbf{C}_{\mathrm{hfeqc}} \\ \mathbf{C}_{\mathrm{hfeqc}} \end{bmatrix}. \tag{A.60}$$

APPENDIX B
SYNCHROPHASORS

This thesis heavily uses the concept of phasor, and more specifically its synchrophasor variant. In this appendix, relevant information about phasors and PMUs is presented alongside the description of the algorithm that was used to convert measurements recorded in the time domain to their synchrophasor representation.

B.1 Introduction and standardization

A phasor is a complex number that represents a sinusoidal waveform, and specifically its magnitude and angle. Each phasor is implicitly associated with the frequency of the corresponding sinusoid. Since phasors are complex numbers, both polar and rectangular representations are frequently used depending the application. Synchronized phasors, also known as synchrophasors, are time synchronized phasors, i.e., timestamped phasors that use a timing signal as a common reference for their angle value [73].

PMUs are either independent devices or modules within devices that convert time domain measurements to synchrophasors based on some estimation algorithm. Since there is an array of algorithms to perform this conversion and PMU circuits can also be physically different from each other, different PMUs might output slightly different synchrophasors under some conditions, so standardization is needed to ensure that synchrophasors from different sources are comparable.

As of the time of this writing, [73] is the main synchrophasor standard having superseded [74] and [75].

Another standard that was extensively used for this thesis is the Common Format for Transient Data Exchange (COMTRADE). Its most recent version available during the preparation of this thesis is in [76], which superseded [77]. The COMTRADE standard introduces a common data format that is suitable for data either directly recorded by measuring devices or produced through simulation. It facilitates the exchange of waveform data between different entities and applications, and can accommodate both time domain measurements and synchrophasors.

B.2 Synchrophasor estimation

In this research work, phasor extraction from time domain samples has been performed using an algorithm presented in the "Power System Protection" course taught during the Spring semester of 2016 by Professor A.P. "Sakis" Meliopoulos at the Georgia Institute of Technology (Georgia Tech). This algorithm is split into a fundamental frequency estimation step and a phasor calculation step.

B.2.1 Fundamental frequency estimation

The fundamental frequency of an AC power system under normal operating conditions may vary within a narrow range around its nominal value. Thus, accurate estimation of the actual instantaneous value of this quantity is very important for a variety of applications including synchrophasor calculation. Here, the rate of change of the phasor angle of a recorded waveform is used to estimate the power system fundamental frequency.

Assume that some quantity within the power system denoted as x is constantly monitored with the i-th waveform sample denoted as $x[i]$. Moreover, assume that the nominal power system frequency is f_0, and the sampling period is T. Then, the number of samples within one period N is defined as

$$N = \left\lfloor \frac{1}{f_0 T} \right\rfloor . \tag{B.1}$$

Now, two accumulators can be defined as

$$V_1[k] = \sum_{i=k-N+1}^{k} x[i] \cos\left(2\pi f_0 T i\right), \tag{B.2}$$

$$V_2[k] = \sum_{i=k-N+1}^{k} x[i] \sin\left(2\pi f_0 T i\right). \tag{B.3}$$

Then, the instantaneous phasor angle is simply

$$\phi[k] = \mathrm{atan2}(-V_2[k], V_1[k]), \tag{B.4}$$

The step angle change can be calculated using the instantaneous phasor angles as

$$\Delta\phi[k] = \phi[k] - \phi[k-1]. \tag{B.5}$$

The step angle change should always be kept within the $(-\pi, \pi]$ range by adding or subtracting 2π, if necessary.

Finally, the instantaneous fundamental frequency is

$$f[k] = f_0 + \frac{\Delta\phi[k]}{2\pi T}. \tag{B.6}$$

While the search for improved algorithms for fundamental frequency estimation continues [78, 79, 80], the algorithm presented here satisfied the computational requirements of the proposed centralized protection scheme. In Section B.2.2, a practical implementation of the accumulators in Equations (B.2) and (B.3) is also presented.

B.2.2 Phasor calculation

Once an estimate $\hat{f}_0$ for the instantaneous fundamental frequency $f[k]$ has been made, the corresponding fundamental angular frequency ω_0 can be calculated as

$$\omega_0 = 2\pi \hat{f}_0. \tag{B.7}$$

Then, the intermediate quantities y and z at step k are calculated as

$$y[k] = x[k] \cos\left(\omega_0 T k\right), \tag{B.8}$$

$$z[k] = x[k] \sin\left(\omega_0 T k\right), \tag{B.9}$$

where T denotes the sampling period again, and x is the recorded waveform. These intermediate quantities help populate the circular buffers of the algorithm presented in Figure B.1.

A circular buffer offers an elegant and computationally efficient method of implementing various algorithms including the phasor extraction algorithm used in this thesis. Specifically, two circular buffers, each of size N, are used as shown in Figure B.1 to update the accumulators defined in Equations (B.2) and (B.3). Both accumulators, as well as each cell of the two circular buffers, are initialized with zeros.

As the k-th recorded value of x is received, $y[k]$ and $z[k]$ are calculated as shown in Equations (B.8) and (B.9). Then, the $y[k-N]$ and $z[k-N]$ are retrieved from the corresponding circular buffers, and the accumulators are updated as

$$V_1[k] = V_1[k-1] + y[k] - y[k-N], \tag{B.10}$$

$$V_2[k] = V_2[k-1] + z[k] - z[k-N]. \tag{B.11}$$

Then, the $y[k-N]$ value in the circular buffer is overwritten with the $y[k]$ value, and

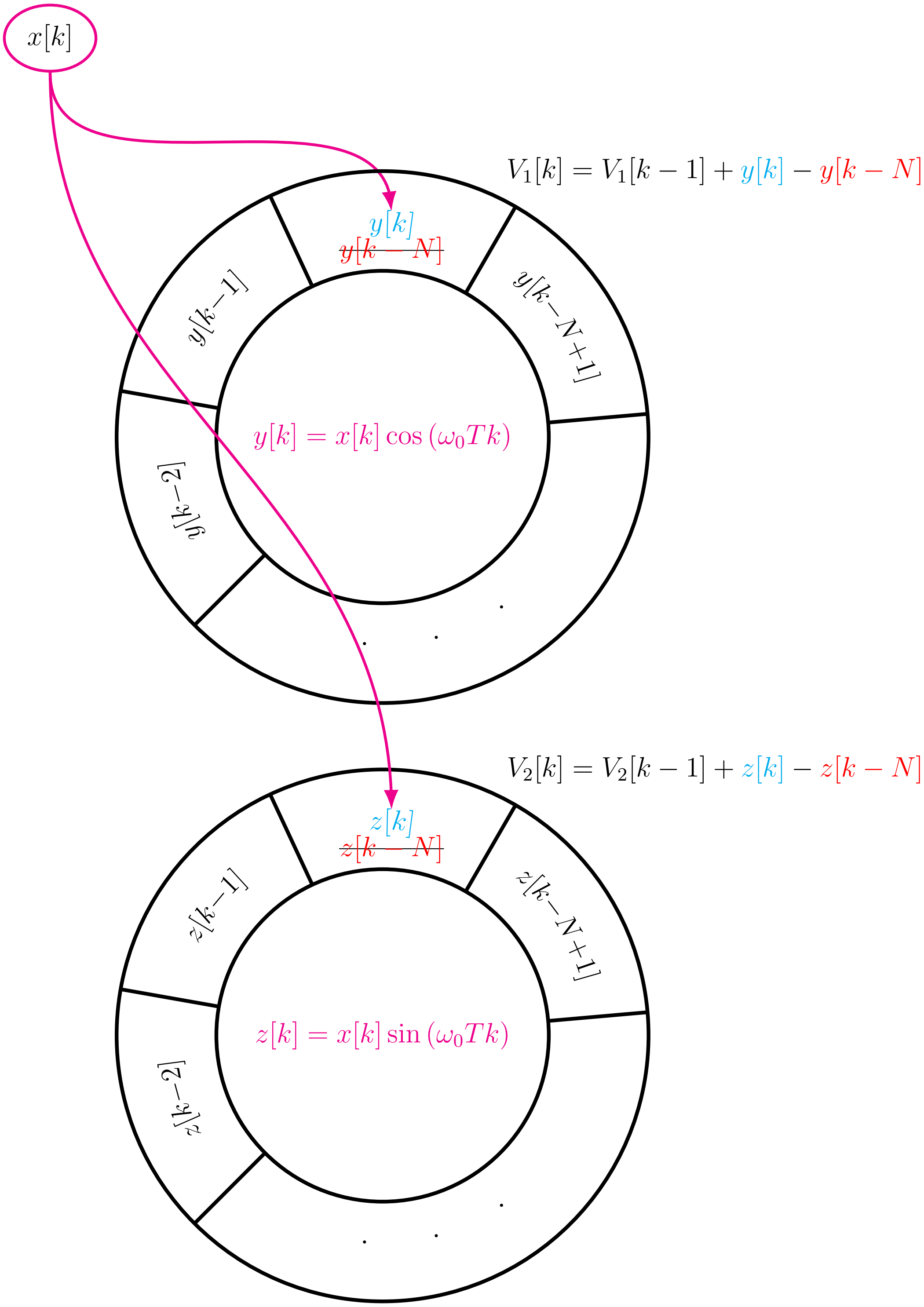
$x[k]$
$V_1[k] = V_1[k-1] + y[k] - y[k-N]$
$y[k]$
~~$y[k-N]$~~
$y[k-1]$
$y[k-N+1]$
$y[k] = x[k]\cos(\omega_0 Tk)$
$y[k-2]$
$V_2[k] = V_2[k-1] + z[k] - z[k-N]$
$z[k]$
~~$z[k-N]$~~
$z[k-1]$
$z[k-N+1]$
$z[k] = x[k]\sin(\omega_0 Tk)$
$z[k-2]$

Figure B.1: Circular array implementation for phasor estimation.

the $z[k-N]$ value is overwritten with the $z[k]$ value.

Finally, the phasor X corresponding to quantity x at step k, can be calculated as

$$X[k] = \frac{\sqrt{2}}{N} \left(V_1[k] + jV_2[k] \right), \tag{B.12}$$

with the corresponding phasor frequency being equal to

$$f[k] = f_0 + \frac{\Delta\phi[k]}{2\pi T}. \tag{B.13}$$

In this thesis, the circular buffers have been implemented as arrays addressed using the modulo operator. Moreover, it should be noted that the initial value for each phasor equals zero, since all accumulators and circular buffers are initialized with zeros. Hence, at least N measurements are needed in order to get an accurate estimate for each phasor. Thus, the proposed centralized protection scheme in this thesis starts operating after the first N samples are processed.

B.3 Implementation details

Based on the standards and the algorithm presented in this appendix, various computer programs were produced using Python, MATLAB, and C++ at different stages of development.

First, a COMTRADE-compatible reader was developed to handle all waveforms produced through WinIGS simulations. WinIGS simulations were performed mainly in the time domain, but there were also some tests in the quasi-dynamic domain to validate the quasi-dynamic models used for DSE. A significant advantage of the COMTRADE standard is that both types of data are read in exactly the same way, which simplifies code development. The output of the COMTRADE reader was used either to plot the graphs of this dissertation or for further analysis.

The synchrophasor estimation algorithm presented above was used to convert time domain waveforms (usually provided by the COMTRADE reader) to their equivalent synchrophasor form.

As part of this research work, a COMTRADE writer was also developed in order to write the calculated phasor waveforms back to COMTRADE files, which was useful mainly for plotting and for debugging purposes. Once more, the exact same writer can also output time domain waveforms in COMTRADE format.

Since one of the characteristics of this research work is an emphasis on modularity and interoperability, any of the above functions can be rewritten without affecting the rest of the codebase. In particular, this was highly important for the phasor estimation part, because different candidate algorithms were considered at the design stage. Hence, the ability to quickly change the way time domain waveforms are converted to synchrophasors without affecting the rest of the execution was very desirable.

B.4 Conclusion and further reading

The most recent IEEE/IEC synchrophasor standard document [73] illustrates the challenges posed to accurate synchrophasor estimation by transients and harmonics. Specifically, one of the criteria to evaluate PMU accuracy according to the standards is its performance under step changes in magnitude and phase. As far as harmonics are concerned, the document explains that they may corrupt the recorded time domain waveform and perplex the effort to estimate its corresponding synchrophasor. For this reason, the standard defines mandatory accuracy limits for any PMU that receives signals with harmonic distortion below some specified thresholds. Thus, it is clear that successful navigation of these challenges is necessary to validate the good performance of any estimation algorithm.

Both of these challenges are important in this thesis.

First, abrupt changes in the magnitude and angle of recorded waveforms such as instantaneous voltages are direct consequences of any power fault. Such faults may unleash various transient responses that challenge the ability of any PMU to accurately calculate and report the corresponding synchrophasor values. FDIAs can also cause sudden waveform changes in order to trick protection schemes into misoperation. Both power faults and FDIAs that induce abrupt signal changes are studied in this thesis for the two presented microgrids.

The algorithm introduced in section B.2 exhibited good behavior when tested with a relatively simplified microgrid such as the one in section 7.1. However, it was not expected that this algorithm would perform equally well with the more detailed microgrid of section 7.2, which included full modeling of the switching behavior of the inverters. Therefore, some other options were examined, which will be presented later in this appendix. Nevertheless, when the algorithm of section B.2 was tested with the more detailed microgrid, it only resulted in some minor oscillations that did not affect the proper operation of the proposed centralized protection scheme. Thus, no other algorithm was implemented for this thesis.

The preliminary exploration of alternative algorithms revealed a very active research area, as the search for new synchrophasor estimation algorithms can be the topic of theses in itself [81]. The challenges regarding abrupt waveform change and harmonics are not the only problems with accurate synchrophasor estimation. Other challenges include aperiodic components (usually decaying DC offsets during transients), and noise [81].

The DFT has been extensively used both to directly estimate synchrophasors, and as a basis for improved algorithms that have even more attractive characteristics such as better accuracy. Such DFT-based algorithms may utilize sampling interval tuning, variable DFT window lengths, iterative changes of the base frequency of the algorithm, gain correction, and recursive weight tuning [82]. Improvements can also be offered through the use of least squares, Kalman filtering or the Clarke Transformation [82, 83, 84].

Other synchrophasor estimation techniques that have been proposed include algorithms based on the wavelet transform, dynamic phasors, Taylor-Kalman, Taylor-Fourier, and Taylor-Kalman-Fourier filtering [82, 83, 85].

The scope of the literature illustrates the importance of fast and accurate synchrophasor estimation for a variety of applications. As applications of the novel protection scheme that is introduced in this thesis may require improved accuracy to operate properly, modularity is an important prerequisite. This is achieved through the object-oriented design of the protection scheme, which means that the current synchrophasor estimation module can be easily replaced with one of the more advanced algorithms presented in this appendix at the expense of additional computational complexity.

REFERENCES

[1] A. Blinder and N. Perlroth, “A Cyberattack Hobbles Atlanta, and Security Experts Shudder,” *The New York Times*, Mar. 2018.

[2] C. McWhirter and J. De Avila, “Atlanta Hit With Cyberattack,” *Wall Street Journal*, Mar. 2018.

[3] “Map: Colonial Pipeline network through metro Atlanta,” *The Atlanta Journal-Constitution*, May 2021.

[4] US Energy Information Administration (EIA), “Cyberattack halts fuel movement on Colonial petroleum pipeline,” *Today in Energy*, May 2021.

[5] J. Carroll, A. Guerra Luz, and J. R. Shah, “Gas Stations Run Dry as Pipeline Races to Recover From Hacking,” *Bloomberg*, May 2021.

[6] J. R. Biden Jr., “Executive Order on Improving the Nation’s Cybersecurity,” *The White House*, May 2021.

[7] C. Bing, “Exclusive: U.S. to give ransomware hacks similar priority as terrorism,” *Reuters*, Jun. 2021.

[8] A. Greenberg, “A Hacker Tried to Poison a Florida City’s Water Supply, Officials Say,” *Wired*, Feb. 2021.

[9] K. Collier, “50,000 security disasters waiting to happen: The problem of America’s water supplies,” *NBC News*, Jun. 2021.

[10] CBS Staff, “Global cyberattack strikes dozens of countries, cripples U.K. hospitals,” *CBS News*, May 2017.

[11] F. Bajak and R. Alonso-Zaldivar, “Cyberattack hobbles major hospital chain’s US facilities,” *The Associated Press*, Sep. 2020.

[12] AP Staff, “Irish health system struggling to recover from cyberattack,” *The Associated Press*, May 2021.

[13] D. U. Case, “Analysis of the cyber attack on the Ukrainian power grid,” *Electricity Information Sharing and Analysis Center (E-ISAC)*, 2016.

[14] Reuters Staff, “Mumbai power outage could have been cyber sabotage, says minister,” *Reuters*, Mar. 2021.

[15] D. E. Sanger and E. Schmall, “China Appears to Warn India: Push Too Hard and the Lights Could Go Out,” *The New York Times*, Feb. 2021.

[16] E. Auchard and C. Steitz, “German nuclear plant infected with computer viruses, operator says,” *Reuters*, Apr. 2016.

[17] D. Das, “An Indian nuclear power plant suffered a cyberattack. Here’s what you need to know.,” *Washington Post*, Nov. 2019.

[18] M. Riley, J. A. Dlouhy, and B. Gruley, “Russians Are Suspects in Nuclear Site Hackings, Sources Say,” *Bloomberg*, Jul. 2017.

[19] J. Finkle, “Malicious virus shuttered power plant: DHS,” *Reuters*, Jan. 2013.

[20] US Department of Energy, “Cybersecurity Strategy 2018-2020,” Tech. Rep., Jun. 2018.

[21] US Department of Energy, “Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats,” *Energy.gov*, Apr. 2021.

[22] European Commission, “Commission Recommendation of 3.4.2019 on cybersecurity in the energy sector,” *Official Journal of the European Union L96*, vol. 62, pp. 50–54, Apr. 2019.

[23] B. Xie *et al.*, “A Performance Comparison Study of Quasi-Dynamic State Estimation and Static State Estimation,” in *2020 IEEE Power Energy Society General Meeting (PESGM)*, ISSN: 1944-9933, Aug. 2020, pp. 1–5.

[24] B. Xie, A. Sakis Meliopoulos, Y. Liu, and L. Sun, “Distributed quasi-dynamic state estimation with both GPS-synchronized and non-synchronized data,” in *2017 North American Power Symposium (NAPS)*, Sep. 2017.

[25] B. Xie, A. P. S. Meliopoulos, C. Zhong, Y. Liu, L. Sun, and J. Xie, “Distributed Quasi-Dynamic State Estimation Incorporating Distributed Energy Resources,” in *2018 North American Power Symposium (NAPS)*, Sep. 2018.

[26] B. Xie *et al.*, “Dynamic State Estimation Based Unit Protection,” in *2019 IEEE Power Energy Society General Meeting (PESGM)*, ISSN: 1944-9933, Aug. 2019.

[27] O. Vasios, B. Xie, and A. P. Meliopoulos, “Estimation Based Protection of Three-Phase Saturable Core Transformer for Cross-Country Fault Detection,” in *Proceedings of 2019 IEEE Power Energy Society General Meeting (PESGM)*, Aug. 2019.

[28] K. Liu, A. P. Sakis Meliopoulos, B. Xie, C. Zhong, and J. Xie, “Dynamic State Estimation-Based Protection of Distribution Systems with High Penetration of DERs,”

in *2020 IEEE Power Energy Society General Meeting (PESGM)*, ISSN: 1944-9933, Aug. 2020, pp. 1–5.

[29] B. Xie, D. Zhao, T. Hong, A. Q. Huang, Z. Guo, and Y. Lin, "Dynamic State Estimation Based Monitoring of High Frequency Transformer," in *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Nov. 2020.

[30] J. C. Lazarte, O. Vasios, and A. Meliopoulos, "Analysis of the operation and power quality of a microgrid with photovoltaic sources," in *2018 North American Power Symposium (NAPS)*, Sep. 2018, pp. 1–6.

[31] M. Zeller, "Common questions and answers addressing the aurora vulnerability," *Schweitzer Engineering Laboratories Technical Report*, pp. 20 150 812–081 908, 2011.

[32] R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," *IEEE Security & Privacy Magazine*, vol. 9, no. 3, pp. 49–51, May 2011.

[33] P. Polityuk, O. Vukmanovic, and S. Jewkes, "Ukraine's power outage was a cyber attack: Ukrenergo," *Reuters*, Jan. 2017.

[34] Wikipedia, *2017 cyberattacks on Ukraine*, Page Version ID: 900376690, Jun. 2019.

[35] S. Simon and B. Sobczak, "'Cyber Disruption' Affected Parts Of U.S. Energy Grid," *NPR Weekend Edition Saturday*, May 2019.

[36] D. E. Sanger and N. Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *The New York Times*, Jun. 2019.

[37] N. Virvilis and D. Gritzalis, "The Big Four - What We Did Wrong in Advanced Persistent Threat Detection?" In *Proceedings of 2013 International Conference on Availability, Reliability and Security*, Regensburg, Germany: IEEE, Sep. 2013, pp. 248–254, ISBN: 978-0-7695-5008-4.

[38] C. Konstantinou, A. Keliris, and M. Maniatakos, "Taxonomy of firmware Trojans in smart grid devices," in *Proceedings of 2016 IEEE Power and Energy Society General Meeting (PESGM)*, Boston, MA, USA: IEEE, Jul. 2016, pp. 1–5, ISBN: 978-1-5090-4168-8.

[39] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in Distributed Power Systems," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1367–1388, Jul. 2017.

[40] Z. Lu, W. Wang, and C. Wang, "Camouflage Traffic: Minimizing Message Delay for Smart Grid Applications under Jamming," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 31–44, Jan. 2015.

[41] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, “A Review of False Data Injection Attacks Against Modern Power Systems,” *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[42] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragicevic, “A Stealth Cyber Attack Detection Strategy for DC Microgrids,” *IEEE Transactions on Power Electronics*, pp. 1–1, 2018.

[43] D. Jin *et al.*, “Toward a Cyber Resilient and Secure Microgrid Using Software-Defined Networking,” *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2494–2504, Sep. 2017.

[44] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, “Signal Temporal Logic-Based Attack Detection in DC Microgrids,” *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3585–3595, Jul. 2019.

[45] M. Chlela, D. Mascarella, G. Joos, and M. Kassouf, “Fallback Control for Isochronous Energy Storage Systems in Autonomous Microgrids Under Denial-of-Service Cyber-Attacks,” *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4702–4711, Sep. 2018.

[46] Shuping Gong, Zhenghao Zhang, M. Trinkle, A. D. Dimitrovski, and Husheng Li, “GPS spoofing based time stamp attack on real time wide area monitoring in smart grid,” in *Proceedings of 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, Tainan, Taiwan: IEEE, Nov. 2012, pp. 300–305.

[47] J. Zhao, L. Mili, and M. Wang, “A Generalized False Data Injection Attacks Against Power System Nonlinear State Estimator and Countermeasures,” *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 4868–4877, Sep. 2018.

[48] A. J. Gallo, M. S. Turan, P. Nahata, F. Boem, T. Parisini, and G. Ferrari-Trecate, “Distributed Cyber-Attack Detection in the Secondary Control of DC Microgrids,” in *Proceedings of 2018 European Control Conference (ECC)*, Limassol: IEEE, Jun. 2018, pp. 344–349, ISBN: 978-3-9524269-8-2.

[49] M. A. Rahman and H. Mohsenian-Rad, “False data injection attacks against nonlinear state estimation in smart power grids,” in *Proceedings of 2013 IEEE Power & Energy Society General Meeting*, Vancouver, BC: IEEE, 2013, pp. 1–5, ISBN: 978-1-4799-1303-9.

[50] Y. Zhang, L. Wang, W. Sun, R. C. Green II, and M. Alam, “Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids,” *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 796–808, Dec. 2011.

[51] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, “Detecting Stealthy False Data Injection Using Machine Learning in Smart Grid,” *IEEE Systems Journal*, vol. 11, no. 3, pp. 1644–1652, Sep. 2017.

[52] U. Adhikari, T. H. Morris, and S. Pan, “Applying Non-Nested Generalized Exemplars Classification for Cyber-Power Event and Intrusion Detection,” *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 3928–3941, Sep. 2018.

[53] Y. Chakhchoukh, S. Liu, M. Sugiyama, and H. Ishii, “Statistical outlier detection for diagnosis of cyber attacks in power state estimation,” in *Proceedings of 2016 IEEE Power and Energy Society General Meeting (PESGM)*, Boston, MA, USA: IEEE, Jul. 2016, pp. 1–5, ISBN: 978-1-5090-4168-8.

[54] E. M. Ferragut, J. Laska, M. M. Olama, and O. Ozmen, “Real-Time Cyber-Physical False Data Attack Detection in Smart Grids Using Neural Networks,” in *Proceedings of 2017 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, USA: IEEE, Dec. 2017, pp. 1–6, ISBN: 978-1-5386-2652-8.

[55] Z. Wang, Y. Chen, F. Liu, Y. Xia, and X. Zhang, “Power System Security Under False Data Injection Attacks With Exploitation and Exploration Based on Reinforcement Learning,” *IEEE Access*, vol. 6, pp. 48 785–48 796, 2018.

[56] S. Kampezidou, O. Vasios, and S. Meliopoulos, “Multi-Microgrid Architecture: Optimal Operation and Control,” in *2018 North American Power Symposium (NAPS)*, Sep. 2018.

[57] K. E. Martin *et al.*, “IEEE Standard for Synchrophasors for Power Systems,” *IEEE Transactions on Power Delivery*, vol. 13, no. 1, pp. 73–77, Jan. 1998.

[58] A. G. Phadke, “Synchronized phasor measurements in power systems,” *IEEE Computer Applications in Power*, vol. 6, no. 2, pp. 10–15, Apr. 1993.

[59] L. Sun, A. Sakis Meliopoulos, Y. Liu, and B. Xie, “Dynamic state estimation based synchronous generator model calibration using PMU data,” in *2017 IEEE Power Energy Society General Meeting*, ISSN: 1944-9933, Jul. 2017.

[60] C. Zhong, A. P. Sakis Meliopoulos, J. Sun, M. Saeedifard, and B. Xie, “Modeling of Converter Losses with High Fidelity in a Physically Based Object-Oriented Way,” in *2018 IEEE Power Energy Society General Meeting (PESGM)*, ISSN: 1944-9933, Aug. 2018.

[61] G. De Carne, M. Liserre, B. Xie, C. Zhong, S. A. P. Meliopoulos, and C. Vournas, “Multiphysics Modelling of Asynchronously-Connected Grids,” in *2018 Power Systems Computation Conference (PSCC)*, Jun. 2018.

[62] C. Zhong, A. P. S. Meliopoulos, B. Xie, J. Xie, K. Liu, and H. Shao, “Detailed Multiphysics Modeling of Air-Conditioned House,” in *2019 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, ISSN: 2472-8152, Feb. 2019.

[63] K. Liu, A. P. S. Meliopoulos, B. Xie, C. Zhong, and J. Xie, “Quasi-Dynamic Domain Modeling of Line-Commutated Converters with the Analytical Approach,” in *2019 North American Power Symposium (NAPS)*, Oct. 2019, pp. 1–6.

[64] A. P. Meliopoulos, G. J. Cokkinides, and G. K. Stefopoulos, “Quadratic Integration Method,” in *Proceedings of 2005 International Conference on Power System Transients (IPST 2005)*, Montreal, Canada, 2005.

[65] G. K. Stefopoulos, G. J. Cokkinides, and A. P. Meliopoulos, “Quadratic integration method for transient simulation and harmonic analysis,” in *Proceedings of 2008 13th International Conference on Harmonics and Quality of Power*, ISSN: 2164-0610, Sep. 2008.

[66] G. K. Stefopoulos, “Quadratic power system modeling and simulation with application to voltage recovery and optimal allocation of VAr support,” PhD Dissertation, Georgia Institute of Technology, Jul. 2009.

[67] A. P. Meliopoulos *et al.*, “Dynamic State Estimation-Based Protection: Status and Promise,” *IEEE Transactions on Power Delivery*, vol. 32, no. 1, pp. 320–330, Feb. 2017.

[68] O. Vasios, S. Kampezidou, and A. S. Meliopoulos, “A Dynamic State Estimation Based Centralized Scheme for Microgrid Protection,” in *2018 North American Power Symposium (NAPS)*, Sep. 2018.

[69] B. Xie, “An object-oriented distribution system distributed quasi-dynamic state estimator,” PhD Dissertation, Georgia Institute of Technology, Jul. 2020.

[70] M. Al Owaifeer, “Microgrid energy management system with ancillary services to the grid,” PhD Dissertation, Georgia Institute of Technology, Jul. 2021.

[71] G. K. Stefopoulos, G. J. Cokkinides, and A. P. S. Meliopoulos, “Quadratized model of nonlinear saturable-core inductor for time-domain simulation,” in *Proceedings of 2009 IEEE Power Energy Society General Meeting*, ISSN: 1932-5517, Jul. 2009.

[72] W. Gao, E. Solodovnik, R. Dougal, G. Cokkinides, and A. P. Meliopoulos, “Elimination of numerical oscillations in power system dynamic simulation,” in *Proceedings of Eighteenth Annual IEEE Applied Power Electronics Conference and Exposition, 2003. APEC ’03.*, vol. 2, Feb. 2003, 790–794 vol.2.

[73] “IEEE/IEC 60255-118-1-2018 - IEEE/IEC International Standard - Measuring relays and protection equipment - Part 118-1: Synchrophasor for power systems - Measurements,” IEEE/IEC 60255-118-1-2018, Dec. 2018.

[74] “IEEE C37.118.1-2011 - IEEE Standard for Synchrophasor Measurements for Power Systems,” IEEE C37.118.1-2011, Dec. 2011.

[75] “IEEE C37.118.1a-2014 - IEEE Standard for Synchrophasor Measurements for Power Systems – Amendment 1: Modification of Selected Performance Requirements,” IEEE C37.118.1a-2014, Apr. 2014.

[76] “IEEE/IEC C37.111-2013 - IEEE/IEC International Standard - Measuring relays and protection equipment – Part 24: Common format for transient data exchange (COMTRADE) for power systems,” IEEE/IEC C37.111-2013, Apr. 2013.

[77] “IEEE C37.111-1999 - IEEE Standard Common Format for Transient Data Exchange (COMTRADE) for Power Systems,” IEEE C37.111-1999, Mar. 1999.

[78] R. Chudamani, K. Vasudevan, and C. S. Ramalingam, “Real-Time Estimation of Power System Frequency Using Nonlinear Least Squares,” *IEEE Transactions on Power Delivery*, vol. 24, no. 3, pp. 1021–1028, Jul. 2009.

[79] Y. Xia, Y. He, K. Wang, W. Pei, Z. Blazic, and D. P. Mandic, “A Complex Least Squares Enhanced Smart DFT Technique for Power System Frequency Estimation,” *IEEE Transactions on Power Delivery*, vol. 32, no. 3, pp. 1270–1278, Jun. 2017.

[80] J. Sun, E. Aboutanios, D. B. Smith, and J. E. Fletcher, “Robust Frequency, Phase, and Amplitude Estimation in Power Systems Considering Harmonics,” *IEEE Transactions on Power Delivery*, vol. 35, no. 3, pp. 1158–1168, Jun. 2020.

[81] P. Romano, “DFT-based Synchrophasor Estimation Algorithms and their Integration in Advanced Phasor Measurement Units for the Real-time Monitoring of Active Distribution Networks,” PhD Dissertation, EPFL, Lausanne, 2016.

[82] J. Ren and M. Kezunovic, “Real-Time Power System Frequency and Phasors Estimation Using Recursive Wavelet Transform,” *IEEE Transactions on Power Delivery*, vol. 26, no. 3, pp. 1392–1402, Jul. 2011.

[83] P. Romano and M. Paolone, “Enhanced Interpolated-DFT for Synchrophasor Estimation in FPGAs: Theory, Implementation, and Validation of a PMU Prototype,” *IEEE Transactions on Instrumentation and Measurement*, vol. 63, no. 12, pp. 2824–2836, Dec. 2014.

[84] L. Zhan, Y. Liu, and Y. Liu, “A Clarke Transformation-Based DFT Phasor and Frequency Algorithm for Wide Frequency Range,” *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 67–77, Jan. 2018.

[85] J. A. de la O Serna and J. Rodríguez-Maldonado, “Taylor–Kalman–Fourier Filters for Instantaneous Oscillating Phasor and Harmonic Estimates,” *IEEE Transactions on Instrumentation and Measurement*, vol. 61, no. 4, pp. 941–951, Apr. 2012.

VITA

Orestis Vasios was born in Athens, Greece.

He received his Diploma in Electrical and Computer Engineering from the National Technical University of Athens in July 2015. In August 2015, he joined the Power Systems Control and Automation Laboratory (PSCAL) at the Georgia Institute of Technology (Georgia Tech) in Atlanta, GA working under the supervision of Professor A.P. "Sakis" Meliopoulos. During his studies at Georgia Tech, Orestis obtained an M.Sc. in Electrical and Computer Engineering in May 2019, and an M.Sc. in Operations Research in May 2021.

Orestis also served as Graduate Research Assistant and Graduate Teaching Assistant at Georgia Tech. From August 2017 until May 2021 he was the instructor for the Circuits and Electronics (ECE 3710) class at Georgia Tech. From May 2020 to August 2020 he interned at the Argonne National Laboratory in Lemont, IL.

Orestis's research interests include power system protection, power system optimization, cyberphysical systems and cybersecurity, and applications of Machine Learning (ML) in power systems. His research work has produced several papers in peer-reviewed publications.